ISSN No:-2456-2165

A Survey on Biometrics as a Security Provider

Vidya More, Sakshi Gavali, Pooja Kale
Department of Computer Science and
Engineering Sandip University Nashik Maharashtra, India

Abstract:- Now days, security of the confidential information of the organization or an individual become a serious issue. Because of vulnerability of system allow to unauthorized person to access the confidential information or data. Because of unauthorized access the confidentiality of information get break. So, biometrics is a good hierarchy to maintain the security of the confidential data. Accordingly, Biometrics refers to the physical and behavioral characteristics of the human, Such as face recognition, voice, gait, finger print, palm retina etc. Correspondingly, by using of biometrics it is possible to establish an individual identity based on "who user is rather than "what he holds or own". In this paper we make a survey on previous biometrics topics, its advantages and disadvantages and related privacy concerns.

Keywords:- *Biometrics, Recognition, Identification, Verification etc.*

I. INTRODUCTION

An ancient contrivance that peoples know each other by their face, voice, gesture, & posture. This are all characteristics for each and every human being so, this characteristics use as authentication password.
Prior to that Biometrics is a computer science provide access control so only authenticate person is able to access the data. The term Biometrics is the combination of two words that are BIO means "life" and METRICS means "measure".
According to previous research we make a survey on various biometric technologies based on their efficiency, usability and their social needs.

A. *Biometrics System*

Radically, Biometrics is a technology use to protect or maintain confidentiality and integrity of the data. Each of human being have there own characteristics like fingers, face, retina, voice, gait, handwriting. [1]

The Biometrics technology accommodates these characteristics of humans as a password authentication. Basically it is a pattern lock system which uses physical and behavioral possessions of human beings. For eg. If one person add finger print to unlock his mobile. If other Un-authorize person try to gain access of that mobile phone he can't access the device because of the finger print is add by authorize person to unlock the device and each person having there distinct fingerprint.

Prior to that biometrics survive through four phases to unlock the system [1]:-

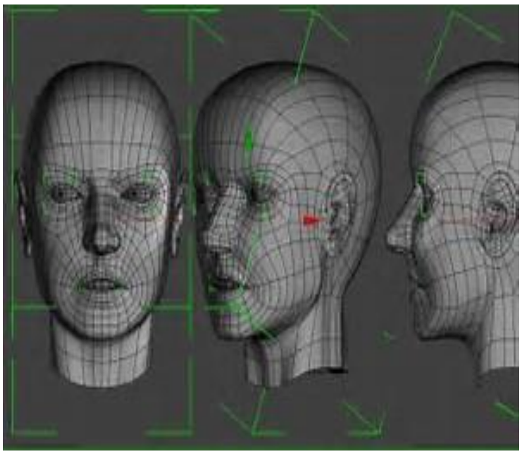
- Feature sensor to recognize the password.
- Person adds his discriminative as patterns to unlock the system.
- When user request to unlock device with the pattern, then internally system will check the requested characteristic is match or not in device.
- If it matches then give access only to authenticate user or if it not match then the system/device will not unlock.

B. *Previous Invented Biometrics*

➢ *Face Recognition*

The technology "Face recognition" is frequently use in Biometric; it is use as a pattern lock for the system. Certainly unauthorized person cannot equip to unlock the system. [2]

When user wants to unlock the system then he request to system, system analyzes his face check the person is authorize or not in database then, if authorized then system give access to that person. For scrutinizing face "Face recognition" scanner is use. Scanner analyzes the face on the basis of face structure, I.e. eyes, eyebrows, lips, nose, and chin.



➢ *Fingerprint*

"Fingerprint authentication" tremendously uses technology in various mobile phones like smart phones and iPhones. [2]

As stated by previous research work an individual person uses his fingerprint near about 110 times to unlock his device.

Each human being have unique fingerprint. As two twins also not have same fingerprints .It is ideal for end-users or give rights only to authorize person.

➢ *Retina*

According to previous research stated that retina scan is most secured biometric to preserve the systems. By virtue of it is not easy to change anyone's retina and also not possible to replicatean anyone's retina.]2]

To identify the authenticate person "Retina scanner" analyzes the structure of blood vessels present in eye.
As long as for scanning of retina retinal scan uses light source which have low intensity and sensor.

➢ *Gait*

The technology which appertains to individual posture furthermore analyzes a person on the base of his walking style is nothing but "Gait recognition"[2]
Radically it is a behavioral biometric so it detects a person through its behavior.

➢ *Palm Recognition*

Emerging biometric technologies are providing more choice and increased accuracy

Allowing authentication by using human palm is nothing but palm recognition technique. Certainly palm contains ridges and valleys, "it is as consonant as fingerprint recognition".

Nevertheless palm recognition required a large area for scanning so it is superior touse a fingerprint authentication.[2]

Remarkably it is bulky and expensive than fingerprint sensors.

Usually, Palm recognition recognized an individual palm on the structure of lines and wrinkles on palm. Relatively it is scan with a low resolution scanner which would be cheaper.

➢ *Voice recognition*

Determine authorize identity by using voice is nothing but voice recognition technique.

Consequently voice is behavioral and physiological characteristic of individual.
According to that system analyzes an authorized person's voice on the basis vocal tracts, size and shape of appendages. [2]

Although voice is use to diagnose authorize person but sound is precisely not clear or appropriate for identification,

By reason of human voice changes according to its increased age and also due to emotional conditions.[2]
Moreover it has one limitation that voice is sensitive due to some factors like background noise.

II. LITERATURE REVIEW

Face Recognition technique is invented by Woodrow bleasoe & Helen wolf in 1965 .It gives accurate result and it required camera as an identifier device, its cost minimum. It identifies authorized face on basis of face structure.

Fingerprint recognition technique is invented by Henry faulds in 1843. Its accuracy is very high. For scanning of finger it requires fingerprint sensor/scanner. It recognized finger on the basis of ridges and valleys.

Retina invented by Curleton Simon & dr.fsadore Goldstein in 1935. This technique is secure and gives accurate and appropriate result. For recognize it requires camera .and identification base on blood vessels and retina in eye.

Voice recognition is invented by Lenny Baum in 1970. It not gives appropriate result due to some factors like background noise. For recognize it requires microphone and identify voice on the basis of vocal tracts.

	Biometrics	Inventor and Year	Accuracy	Cost	Device required	Identification based on	Social need
1	Face recognition	Woodrow bleasoe & Helen wolf (1965)	High	Medium	Camera	Face (eyes,eyebrows,nose,lips,chin)	high
2	Fingerprint	Henry faulds (1843)	High	Medium	Scanner	Finger (ridges and valleys)	High
3	Retina	Curleton Simon & dr.fsadore Goldstein (1935)	High	High	Camera	Eyes (retina and blood vessels)	Low
4	Palm recognition	-	Medium	Medium	Scanner	Palm (ridges, valleys ,lines wrinkles)	Low
5	Gait	Christian Ottofischer (1980)	Medium	Medium	Scanner	Body (posture walking style)	Low
6	Voice recognition	Lenny Baum (1970)	Medium	Medium	Microph one	Voice (vocal tracts)	High

Table 1- Critical Analysis of Biometric Techniques

III. UTILIZATION OF BIOMETRICS

Application of "Biometric" is divided into three main groups

A. Commercial

Application such as security of Electronic data, ATM, Internet access, Physical access control, PDA, E-commerce, Network login etc.

B. Government

Application such as Correctional facility, National ID cards, Driver's license, Passport control, Social security etc.

C. Forensic

Application such as Criminal investigation, Terrorist identification, Corpse identification, parenthood determination, missing children etc.

- Traditionally Commercial applications are knowledge based systems. For example, it uses PIN and Passwords.
- Government applications uses token based approach. For example, ID cards and badges.
- Forensic applications depends on human expertise to analyze biometrics.

IV. BENEFITS OF BIOMETRICS

➢ *Identification of authorized personality*

Every person have unique biological characteristics like fingerprint and retina. On the basis of this characteristics, User or organization can protect their confidential data from unauthorized access. And this characteristics offers unique and accurate identification method. Biometric is a feature which cannot easily replicate, it means that only authorized person have the right to access the data.

➢ *Accountability*

Biometric gives complete liability to access system or device safely. Scrutinized that biometric cannot easily replicate and also everyone have different characteristic .It is expressively accessible in case of security breaches.

➢ *Straightforward and Safe*

As society needed straightforward and safe systems or devices, so biometric is a technique which gives protection to systems.

Moreover, software and hardware of biometrics are use easily and without any excessive training.

➢ *Convenience*

It considered as convenient security solution, because every person not able to remember passwords and PIN every time, Prior to that using of Biometric technology it not need to remember passwords ,and without credentials we keep our device safe and protected.

V. LIMIRTATIONS OF BIOMETRICS

Moreover, System operates using single biometric characteristic have some limitation

➢ *Limitation about voice recognition*

Voice is not clear and appropriate for identification. According to human increasing age,

Its voice also changes. Voice recognition system also sensitive to factors like background noise.

➢ *Variation*

For authentication, system acquired biometric data of individual and compare with previously add biometric characteristic .If it doesn't matches then system or device will not unlock.

Either if authorized person request to unlock but device not give access the there may be variation, typically caused by user who incorrectly interact with sensors.

Someone expert who better understand this technology this technology can fabricate a copy from the owner's biometric information and gain the access of the system.

VI. CONCLUSION

The technology “Biometrics” introduce to unique identification of a person by evaluating biological traits. Consequently, exclusive identifiers comprises fingerprint, face recognition, retina, voice recognition, gait palm recognition etc.“Retinal scanning” is most secure and safe biometric. Because it not easy to replicate. Most frequently fingerprint recognition is use in devices.“Voice recognition” also used but it is sensitive to background noise, uncertainly it is not very accurate.

Accordingly, “Palm recognition” requires big surface so better of using fingerprint recognition for authentication. So better of using fingerprint for authentication. Overall “Biometrics” is straightforward, simple, easy to use technology and as a privacy concern it permits safety to devices and protect against unauthorized access.

REFERENCES

[1]. Anil K. Jain, Department of Computer Science and Engineering, Michigan State University,”An Introduction to Biometric Recognition1”Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2]. Bhavana Dobriyal ,” reference of various biometrics technologies”.

[3]. S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and Privacy Concerns”, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

[4]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY, 2003.

[5]. Brown, Chappell. Self-contained Fingerprint IDs Forgo PCs, Networks. Electronic Engineering Times,Dec. 14, 1998 p 61.

[6]. Dawley, Heidi. A Program That Never Forgets a Face. Business Week, Dec. 21, 1998 p81.

[7]. For Your Eyes Only: Biometrics. The Economist, Feb. 14, 1998 v346 n8055 p80.

[8]. Hooman Bassirian. Passwords Could Be Past Tense by 2002. Computer Weekly, November 26, 1998.

[9]. McCooey, Eileen. Security Becomes a Priority. Compaq, Dell, others adding security hardware to PCs. Windows Magazine, January 1, 1999.

[10]. Phillips, Ken. New Options in Biometric Identification. PC Week, Sept 7, 1998. v15 n36. p95.