Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

A National Conference On Spectrum Of Opportunities In Science & Engineering Technology
Volume 5, Special Issue 06, April-2018 (UGC Approved)

GLOBAL NEXT GENERATION BIOMATRICS TECHNOLOGY

Shubham Dhanokar[1], Shraddha Shegokar[2], Sanket Dhanokar[3], Harshada Dhanokar[4]

[1]*Computer Science And Engineering, STC, SERT , Shegaon*
[2]*Computer Science And Engineering, STC, SERT, Shegaon*
[3]*Computer Science And Engineering, STC, SERT, Shegaon*
[4]*Computer Science And Engineering, STC, SERT, Shegaon*

Abstract —*The global next generation Biometrics Technology market which highlights the latest technological improvements and new launches current industrial affairs and development. This technological system uses information about a person to identify that person. Biometrics verification is any means by which a person can be uniquely identifiers includes fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA and signatures. The oldest form of Biometrics verification is fingerprinting. Historians have found examples of thumbprints being used as a means of unique identification on clay seals in ancient china. The application of Biometrics technology is include secure access to building, computer system, laptops, cellular phones and ATM's.*

Keywords-*Fingerprint recognition, iris and retina recognition, voice recognition, face recognition and the latest technologies like behavioral recognition.*

I. INTRODUCTION

Biometrics based solution are able to provide for confidential financial transaction and personal data privacy. The need for biometrics can be found in federal, state and local government in the military and a commercial application. Enterprise- wide network security infrastructure, government ID's, secure electronic banking, investing and other financial transaction and health and social services are already benefiting from these technologies.

It is fully depends on automated methods of recognizing a based on a physiological or Behavioral characteristics. Among the features measured are face, fingerprint, Hand geometry, iris, retina, signature and voice. It's based authentication application include workstation, networks and domain access signal sign-on, application logon, data protection, remote access to resource transaction and security or most important for wed security.

Security field uses three different types of authentication:

1) Sometimes you know- a password, pin or piece of personal information.
2) Sometimes you are (a biometrics)
3) Sometimes you have – a card key, smart card(like secure and ID card)

It is so important for security purpose.

I. FACIAL RECOGNITION

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database. This technique has attracted considerable understand its capabilities, some vendors have made extravagant claims-which are very difficult it not impossible, to substantiate in practice – for facial

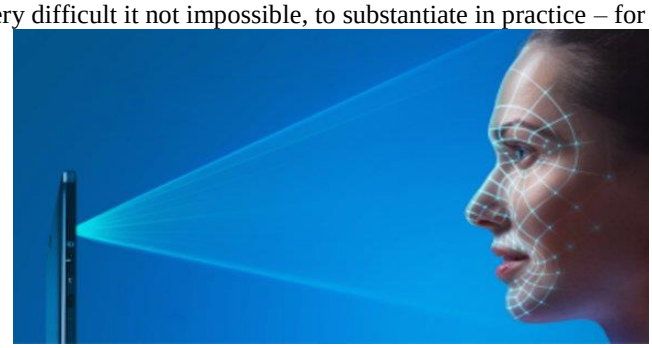

Fig 1:- Facial Biometrics

recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic PC's it is more niche market to network authentication.

II. RETINA

A biometrics identifier known as a retinal scan is used to map the unique patterns of a person's retina .The human retina is a thin tissues composed of neural cell that is located in the posterior portion of the eye almost the person have

its own retina having complex structure but the even identical twins do not share a similar pattern of retina the blood vessels within the retina absorb light more readily that the surrounding tissues and easily identified with appropriate lighting.

1) The retina is a thin layer of cells at the back of the eyeball of vertebrates
2) It is a part of the eye which converts light into nervous signal
3) 3 .The retina consists of multiple layers of sensory tissue and millions of photoreceptors whose function is to transform light rays into neural impulses
4) Two distinct types of photoreceptors exist within the retina: the rods and the cones while the cones helps us to see different colors.

Fig 2 :- Retina

A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. The beam of light traces a standardized path on the retina. Because retinal blood vessels are more absorbent of this light that the rest of the eye, the amount of reflection varies during the scan and its codes stored in a databases.

The retinal scanning also has medical application .communicable illness such as AIDS, syphilis, malaria, as well as hereditary diseases like lymphoma and sickle cell anemia impact the eye.

III. IRIS

The iris, the circular colored membrane surrounding the eye's pupil, is complex enough to be useful for recognition. The performance of system using this modality is promising. Although early systems required significant user cooperation, more modern system are increasingly user friendly. However , although systems based on the iris have quit good FMRs, the FNMRs can be high .further ,the iris is thought to change over time, but variability over a lifetime has not been well characterized the eye related biometrics , users a fairly conventional camera element and requires no close contact between the users and the reader. In addition, it has the potential for higher than average template matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas a new products emerge.

Fig 3 :- Iris

IV. SIGNATURE

Signature verification analyzes the way a users signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction –related identity

verification , and most would see nothing unusual in extending this to encompass biometrics. How a person sign his or her name typically changes over time. It can also be strongly influenced by context , including physical conditions and the emotional state of signer. Extensive experience has also shown that signature are relatively easy to forget. Nevertheless, signatures have been accepted as a method of recognition for a long time.

Signature verification devices are reasonably accurate in operation and obviously lend themselves to application where a signature is an accepted identifiers. Surprisingly relatively few significant signature application have emerged compared with other biometrics methodologies . But if your application fits, it is a technology worth considering

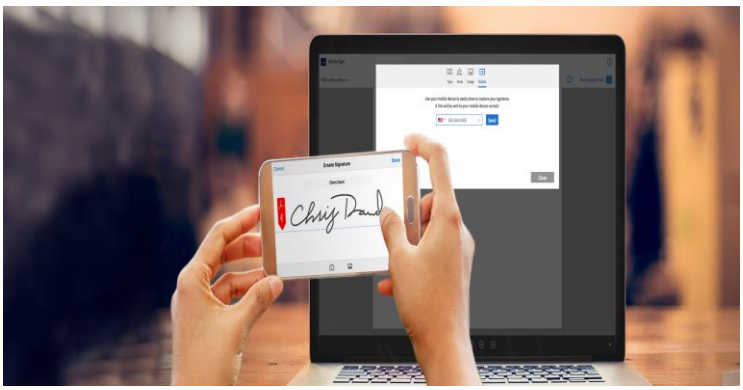

Fig 4 :- Sign

V. FINGERPRINT

Biometrics is a very strong authentication mechanism as it based on something that you are as opposed to something you know or something you have. . A weak or compromised password is the primary reason for the rising cases of security and data breaches Passwords and tokens are highly vulnerable to being lost or stolen. Passwords are the weakest link in an organization's security system and even strong passwords cannot resist sophisticated hacker attacks. Further, the costs of maintaining password and token based systems are very high and inefficient. Resetting lost or forgotten passwords takes up IT support time and reduces employee productivity.

Fingerprints are inherent to individuals and can neither be lost nor stolen which makes it highly accurate and reliable. Moreover, the availability of low-cost fingerprint readers coupled with easy integration capabilities has led to the wide spread deployment of fingerprint biometrics in a variety of organizations.

Verification and identification are the two ways in which an individual's identity can be determined using biometric technology. Verification confirms that a person is indeed who they claim to be and performs a one-to-one comparison of the individual's fingerprint sample with a stored reference template

An organization can enjoy limitless benefits by correctly deploying biometric technology. Fingerprint technology can benefit organizations in a variety of sectors such as health care, government, retail enterprises, technology organizations, manufacturing industry, libraries, universities etc.

Employee identification and workforce management becomes faster, accurate and more efficient with fingerprint technology. Unlike magnetic strip cards or passwords, individuals always carry their fingerprints with them and they cannot be lost or forgotten. A biometric system enables automated calculation of employee hours thus reducing paper wastage and time spent in manual reconciliation of attendance data. Fingerprint biometrics can provide both physical access to company buildings and logical access to internal resources such as enterprise computers and systems.

Governments and organizations all around the world are choosing biometric technology to combat identity fraud and security breaches, secure confidential data, reduce costs and to improve overall user experience. Biometrics is one of the rapidly growing fields in the information technology sector with fingerprint recognition

Fig 5 :- Fingerprint

CONCLUSION

In this technology, we methodically inspected research in regards to cloud computing security so as to recognize the significant security issues this innovation confronts today. In summary, as Biometrics allow for increased security, convenience we can say that fused biometric authentication system will be novel solution for authenticating users on cloud computing ,which can be provided as service on cloud and can be used as a single sign on.

REFERENCES

[1] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, **Handbook of Fingerprint Recognition** (recommended)
[2] John D. Woodward Jr., Nicholas M. Orlans, Peter T. Higgins **Biometrics**
[3] Julian D. M. Ashbourn Biometrics: Advanced Identify Verification: The Complete Guide
[4] Samir Nanavati, Michael Thieme, Raj Nanavati Biometrics: Identity Verification in a Networked World