STUDY OF HUMAN BEHAVIOUR USING BIOMETRICS

Dr.J.Rajeswari[1]

ABSTRACT

Owing to the rapid growth of Information Technology, security has become a prime issue. Nowadays, biometrics plays a vital role in identifying a human's action that can present a threat to security applications like accessing a secure building or a system. Biometrics is used for identifying human's exclusive physiological, behavioural and morphological features to offer special visual recognition. Biometrics is a computerized method to identify a person or verify his uniqueness based on physiological characteristics. It has the ability to consistently differentiate between an authorised person and a shark.

The systems that are currently available are fingerprints, handprints, iris and retina patterns, face recognition and the number of systems that are close to biometrics is voices, signature and keystroke systems. In a few years, the use of biometrics will grow rapidly and turn it much more effective. Biometrics provides a new generation of security services to identify individuals based on the unique identification and measurable patterns in human activities. It is fast, easy to apply, precise, steadfast and a less expensive way of authentication for a variety of applications. This paper elucidates how biometric works and introduces some of the new technologies that make it possible. This paper also looks at the real-world applications of biometrics.

KEYWORD : Biometric, Pattern, Biometric Identification, Biometric Applications.

INTRODUCTION

Biometric authentication is safer than other methods, and ties an identity to a selected individual as an alternative of a password or a code that would be employed.

● Users are often enrolled within the background during a couple of normal interactions. Behavioural biometrics is totally frictionless and does not slow down, disrupt or otherwise interfere with the user experience.

● There are dozens of knowledge points collected, and any combination of them is often used to identify a user; the identification is accurate and precise and users cannot impersonate.

● Authentication happens throughout the whole transaction, and behavioural biometrics provides powerful security against insider intimidation and account takeover as a fraud.

Behavioural biometrics does not replace the password or other legacy sorts of identify authentication. But, it reduces the burden placed on them to picket sensitive data. Even the strongest password is only secure so long as it is secret. By offering a further, continuous layer of identity declaration, behavioural biometrics prevents the password from being one point of security collapse.

Every person possesses certain unique features in terms of both physical and behavioural descriptions that are different from those of everybody else on earth. The most common thing that comes to mind when speaking of unique features is the fingerprint, which is a physical characteristic. But there are other characteristics like the way we write our signature. Together, these sets of characteristics are used to recognize confidentiality with a low-cost level of confidence, and may spectacularly improve the extent of security. Passwords, PINs, smart keys, smart cards and the like are widely used forms of authentication, but have limitations and vulnerabilities. For instance, passwords and

[1]*Assistant Professor*
Department of CS, CA & IT
Karpagam Academy of Higher Education

PINs can be easily forgotten, hard to remember, or stolen. Smart keys can be easily lost or duplicated. Smart cards with magnetic strips can be forged. But a person's biometrics or biological traits cannot be stolen, forgotten or misplaced. As a result, they are way safer and unswerving thanks to authenticate privacy compared to other methods.

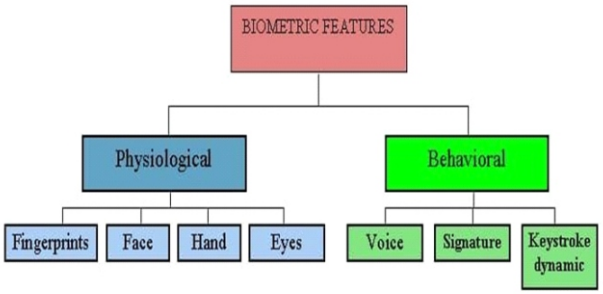

Fig.1: Types of Biometrics

HISTORY OF BIOMETRICS

Authenticating specific seals with fingerprint were carried out by the Chinese emperor Ts'In.

The primary ladder in scientific policing was used and the dimensions were engaged by definite policing by Bertillon A technique that often-proved fool-proof to identify habitual offenders used dimensions taken from explicit anatomical quality, though without contribution of any real assurance of trustworthiness.

The promising use of biometrics was given up, and then rediscovered by James Herschel, a British representative. But it was worn for a completely diverse purpose. He made his subcontractors who built roads in Bengal to sign contracts with their fingerprints. This biometrics authentication was considered the easiest way of finding them more quickly in case of default.

The Metropolitan Police went full swing in utilizing the biometrics for recognition in U.K.

It was initiated by the police and by the FBI in 1924. The French law enforcement also began to begin a comparable process. Telecommunication using Morse code with dash and dots was another means of secure exchange of information during the world war.

An equally effective method was used to spot senders and authentication messages they received by allied forces.

To spot an individual supporting certain unique characteristics is the essential principle of biometrics. Biometric is rising fast, predominantly within the field of uniqueness of documents and combines other safety technologies like elegant cards.

DIFFERENT TYPES OF BIOMETRICS

Types of biometrics are :

1. Fingerprint
2. Facial identification
3. Voice detection
4. Iris detection
5. Retina Scan
6. Keystroke Dynamics
7. Signature acknowledgment

FINGERPRINT

One of the oldest and most developed sorts of biometric recognition is the fingerprint recognition. Fingerprints are verified by comparing the unique loops, arches, and whorls in each pattern, which is easy to capture. Using the image captured, sophisticated algorithms generate exceptional biometric patterns. The template is then compared to new or active scans to either validate or refuse a game.

FACIAL RECOGNITION

Software processes the geometry of the face, counting the space amid the eyes, the space starting from the jaw to the brow, and multiple other points on a person's face for facial recognition. A complicated algorithm transforms the collected information into an encrypted facial signature.

VOICE RECOGNITION

Physically speech, as well as the tip, jaws, and larynx, determines a person's oral swathe. Behaviourally, it means an individual shows some movement variation, nature, tempo and accent, which are additional unique features of identity of every individual. The important properties used in speech authentication are nasal tone, fundamental, and variety. A precise accent print is created by combining data from physical and behavioural biometrics.

IRIS RECOGNITION

The ring-shaped highlighted portion of a person's eye is called iris. The authentication is prepared from many asymmetric fat string-like structures. These gear- like structures of the physique help to adjust the figure of the trainee and allows only a certain amount of sunshine into the eye. By measuring the unique folds of the muscles, biometric identification tools confirm identity with an incredible accuracy. Liveners recognition requires a user to wink to be examined, which adds an additional sheet of exactness and security.

RETINA SCAN

Retinal scans confine the capillary cavernous with the attention by using unique infrared cameras. At first the unrefined picture is pre-processed to increase the image and then process again for the biometric stencil to be used throughout, for verification.

KEYSTROKE DYNAMICS

A person pursues an exact blueprint as typing on the ivories or keypad. These keystroke tempos are often used to start a biometric sketch, which may be used to identify or authenticate a person. The time occupied to push each key, suspension among key presses, lettering type per second and a number of other processes are used to get the keystroke profile of a user. After adding the keystroke dynamics, password-based security can be improved manifold without introducing any lengthy complexity.

SIGNATURE RECOGNITION

Signature recognition is also a sort of biometric method used to analyse the physical activity of signing by measuring special coordinates like pen pressure, stroke order, inclination, and speed. The measurements are digitally recorded, then the information is employed to automatically create a biometric profile for expectations authentication.

APPLICATIONS OF BIOMETRIC BEHAVIOUR

➢ **PHYSICAL SECURITY**

Biometric campaign cannot rule the access to office, laboratories, server rooms, secret building, etc. or intime presence application:

- **Access Control**

The corporeal admission to a room is guarded using fingerprints. This appliance has the dual benefit of ensuring an exceptional safety and not allowing unofficial access of users. When compared to usual keys, biometric access manage eases revoke the user the admission authorization, with no altering the security device.

- **Time and attendance**

It substitutes the classic card clock in and out with a biometric confirmation, with the noticeable benefit of eliminating "buddy-punching".

➢ LOGICAL SECURITY

Biometric devices are second-hand to organize the entrée to altered kinds of possessions such as computer, network, database, websites and documents:

- **Log on to a PC or Network**

Logon to one PC or a network via fingerprints rather than clumsy and unsafe passwords. This is the disadvantages of using biometric technique as a substitute of passwords or badge.

- **Password Bank (Single Sign –on)**

These days, all mainframe users have to memorize not only the logon password, but numerous other passwords that are essential to permit different system assets. Single sign up allows the user to store all the passwords with high security; the website for an instance, requires to include a secret code, that the organism identifies the user's summary and necessitates a biometric verification: once the user uniqueness has been confirmed, the organism reliably provides the exact code word to the website.

- **Remoter Authentication**

Explosion of the global network has intensified the curiosity in the electronic trade. These applications allow distant admission propertyfor each kind. Even it offers enormous opportunity, it is dangerous to underestimate it. The region where there is a robust necessitate for protection; frequently it's essential to authenticate the individuality of a punter on internet when he is associated to an internet spot offer for some quite provision. Password are not a secure resolution as they will be stolen or pooled amid subsequent users. Biometrics is an innate elucidation to distant confirmation. Amongst the applications which nowadays we can really promote are:

- habitat bank, E-Trading
- admission to distant files or spread databases
- sheltered upload of papers in distant collection
- commerce to commerce e- commerce
- Digital Signature

Numerous countries have introduced the rules which make digital autograph lawful price so, fine aid to the dispersal of the lots of fresh applications, by shifting the way of a number of general tasks that are performed now. The digital certificate required for digital name are unrestricted, by guarantee establishment, within elegant Cards are examples. Digitally sign a paper require possessing a sensible licence and therefore the information of the password which typically protect the credential store within the cardboard. Certainly, these two fundamentals aren't sufficient to consider that who is digitally signing a manuscript is really the certified character; actually, the open-end credit with the password can be stolen or merely rented. To allow the license store within the certificate is the only safe way to authenticate the user distinctiveness by using biometrics.

- **Protect and secure the exchanges of document**

The appliance consists of storing entry permit during a cosseted library and prevent, by using fingerprint acknowledgment, any illegal admittance. This type of defence is especially helpful when the certificate has been extracted from the processor and stored somewhere else or has got to be sent by electronic post over an unsecured Internet.

➢ GOVERNMENT APPLICATION

Traditionally, the world first employed the biometrics using fingerprints.

Biometrics is being measured with improved significance to extend safety beside intimidation and struggle unlawful immigrations. Worldwide, quite a few projects are prepared to accept biometrics for private recognition.

The main applications are:

* AFIS for immoral recognition
* social AFIS to keep away from numerous concessions of advantages beneath fraud identity
* safety assurance
* Traveller control at margins
* Control of banned immigration
* Passports and VISA cards

➢ **INTEGRATION INTO THIRD PARTY DEVICES**

More complex devices are often integrated to biometrics, which offers them the likelihood of reliable way of identifying their user. The biometric model should be: 1) completely independent, 2) with an accessible and inclusive crossing point, 3) tiny range, 4) elevated performance and 5) low-priced. Some probable applications are:

* gate curls, resistant doors, stimulating curls
* panic system, gateway openers
* protected boxes, Racks
* ATM, kiosk,
* industrialized equipment
* lorry mechanism, protectorate alarm

UTILIZES AND BENEFITS

The benefits of the biometric technologies are full-bodied, risk-pertinent individuality verification and anti-fraud process, which requires no particular hardware or supplementary safety measures.

➢ Flexibility – Behavioural features are available for analysis of virtual limitless array, and the selected features are often easily tailored to specific needs.

➢ Convenience – Behavioural biometrics analyses the properties of a user device, without distracting the user experience.

➢ Efficiency – The real time application of behavioral biometrics for an identity authentication is legacy authentication mechanism like password entry. The analysis of behavioural biometrics will reduce the time needed to spot and identify the fraud from legitimate user behaviour.

➢ Security –The intrinsic characteristics of behavioural biometrics are very useful to identity the replicate, which is impossible for humans to discern.

CONCLUSION

Biometrics systems have stood alone and proved successful on the technical level as well as on reservoir of experience. The manual method of technical level for identification could be replaced, which is not feasible. Presently, behavioural biometrics is envisioned as an additional layer for authentication and fraud detection systems. Due to availability of sensor to collect behavioural data, the performance of behavioural biometrics could be restricted. Due to the growth of behavioural data with ubiquity and sensitivity of device, the accuracy also gets increased. The potential behavior of biometrics, which is wide-spread and user-friendly, will increase the high-performance identity authentication technology.

REFERENCES

1. A.K. Jain, Next Generation Biometrics, Department of Computer Science & Engineering, Michigan State University, Department of Brain & Cognitive Engineering, Korea University, December 10, 2009
2. Anil Jain (2008): Microsoft Encarta 2008. © 1993-2007 Microsoft Corporation. All rightsreserved. Contributed by; Anil Jain
3. Azeez Y. K. (2001): Personnel Management Ilorin, Olad Publisher. Ilori
4. BehavioSec, Accuracy Report for Native Mobile Application
5. BehavioSec, BehavioWeb: A Case Study of BehavioWeb ia a Real World E- banking Environment

6. BehavioSec, Lifting the lid on Digital Behavior: The Discrepancy between our Online and Offline Selves

7. Defense Advanced Research Projects Agency (DARPA) - Active Authentication Program: Program Page:

8. Gross, S. J., & Niman, C. M. (1975). Attitude-behavior consistency: A review. Public Opinion Quarterly, 39(3), 358–368.

9. K. Shlizerman, R. Basri, 3D Face Reconstruction from a Single Image Using a Single Reference Face Shape, IEEE TRANSACTIONSON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 33, NO. 2, FEBRUARY 2011

10. Leidos Corporation, User Behavior Analytics: The Key to Detecting Insider Attacks,

11. Novetta, Improving Authentication Mechanisms for Enterprise Information System

12. TwoSense, Inc., Mobile Authentication using Device Motion Characteristics,