Biometric system

Submitted by-

Name- Gaurav Sarma

Department- School of computer science and science and Engineering

Lovely Professional University

Phagwara Punjab

Email- gauravsarma68@gmail.com

Name- Divya Thakur

Department-School of computer Engineering, Assistant Professor

Lovely Professional University

Phagwara Punjab

email- divya.28300@lpu.co.in

ABSTRACT

Nowadays, biometric are becoming the preferred solution to a wide range of problems involving identity checking. Biometrics are claimed to provide more secure identification and verification, because 'the body does not lie. Biometrics have the possibility of providing strong security and authentication methods compared to traditional password-oriented security measures. Biometric security technology relies on who you are rather than what you know, in contrast with knowledge-based security. While biometrics has the potential to increase security significantly, it also presents unique drawbacks. In addition, there are underlying normative assumptions regarding human bodies that affect the functioning of biometric systems in highly problematic ways. In recent social science studies, the failures of biometric systems have been interpreted as gendered and racialized biases. A more nuanced understanding of how biometrics and bodily differences intersect draws attention to how bodily differences are produced, used, and problematized during the research and design phases of biometric systems, as well as in their use. In technical engineering research, issues of biometrics performance and human differences are already transformed into R&D challenges in variously more and less problematic ways. In daily practices of border control, system operators engage in workarounds to make the technology work well with a wide range of users. This shows that claims about inherent whiteness of biometrics should be adjusted relationships between biometric technologies, gender and ethnicity are emergent, multiple and complex. Moreover, from the viewpoint of theorizing gender and ethnicity, biometrics difficulties in correctly recognizing pre-defined categories of gender or ethnicity may be less significant than its involvement in producing and enacting gender and ethnic classifications and identities.

INTRODUCTION

The word Biometrics comes from the Greek word's bios meaning life and metrics meaning measure. It refers to a science involving the statistical analysis of biological characteristics. Biometrics the automated recognition of individuals based on their physical and behavioral characteristics such as fingerprints, faces, iris patterns, or voices is quickly becoming central to the exercise of citizenship in countries worldwide. In order to duck the problems of fail to recollection the keywords and ID codes, Biometrics based verification helps us in verifying your finger prints, iris design and voice for your uniqueness at ATM's, Airports etc., you can solve your families, withdrawing money on or after a bank with just a flash of an eye, a tap of your finger or by disinterested presenting your expression.

Biometrics denotes to the unconscious credentials of a person based on his/her physical or behavioral appearances. This technique of identification is preferred over traditional methods concerning passwords and PIN numbers for various reasons:

(i) The being to be recognized is obligatory to be actually existing at the detail of credentials.
(ii) Credentials based on biometric techniques avoids the prerequisite to recollect a PIN or carry a token. By substituting PIN's, biometric methods can actually stop unauthorized admission to or fake use of A.T.M's, Keen cards, PC networks.
(iii) PIN's passwords might be elapsed, and token-based approaches of identification like keywords and driver's licenses might be phony, embezzled or lost. A biometric organization is mainly a pattern obligation scheme which makes an individual identification by important the

authenticity of a precise physiological or social characteristic prejudiced by the user.

LITERATURE REVIEW

There has been much study on the usage of biometric devices and applications, user's attitudes toward such devices, and measurements of impact on performance. Performance gains are often the most significant incentive for adopting a new technology. In relation to this study, the use of biometrics in place of the commonly used passwords could potentially increase performance and security, but user acceptance is the key to its success. With innovative technologies such as biometrics, user acceptance needs to be an equally important factor as usefulness and convenience. Acceptance is also more complex than perceived usability, as it involves social, organizational, and cost factors. Many people have an aversion to learning and accepting new technology or may consider it too inconvenient. There are some potential barriers to acceptance of biometric devices and systems is the perception that they are too intrusive compared to using personal passwords. Biometric security is based on who you are physically, rather than what you know, which is fundamental to its heightened security potential. However, some people feel that allowing a device to read their physical person is providing too much information that is not necessary and could potentially fall into the wrong hands for subversive or illegal purposes. Kat Krol et al. performed a study on facial recognition biometrics as an alternative to the CAPTCHA matching system used by many online ticket sites to determine whether a transaction is conducted by a human, or a bot. CAPTCHA is a favored device used by ticket agencies to prevent unauthorized mass purchases of tickets that could later be scalped for much higher prices. Social and cultural concerns can be another barrier to biometric technology acceptance. In some areas of the world, it is common to avoid any publicly used device, such as a biometric fingerprint scanner. In a cultural study of biometric use, found that the majority of Arab respondents were willing to provide information such as personal passwords, fingerprint scans, and PINs. However, for certain Asian respondents, the willingness to provide this type of information was below 50%, especially with scans of physical or personal characteristics such as voice recognition. In America, Amish communities are culturally and religiously opposed to technology. State requirements to have pictures on their driver's licenses or traffic safety devices on their horse drawn carriages have proved a challenge. In a European study, concluded that users tended not to see big advantages of biometrics over authentication mechanisms such as passwords and PINs, despite improved security. They found that general awareness regarding biometrics needs much improvement, which may also drive more widespread social acceptance of the technology.

METHODOLOGY

This study makes use of quantitative research methodology, applying statistical and numerical analysis to data collected through an Internet browse and taking reference from books. The online search also finds data from around the world and find some useful from there. And currently let's see some of these biometric strategies, their services, compensations and difficulties in detail.

Fingerprint recognition:

Fingerprints are exclusive to each discrete
and no two fingerprints are similar.

Fingerprints comprise designs of edges and valleys as well as niceties points. Minutiae points are occupant edge characteristics that transpire at either the ridge bifurcation or a ridge finish.

There are three methods for perusing fingerprints:

(1) Optical scanners,

(2) Updraft scanners and
(3) Capacitance (solid state) scanners
Now, here are two acknowledged methods for good-looking out the impression data
(I) Minutia-based and
(II) Correlation-based
Minutia-based is the tinier of the two. This method suggestions the ridge physiognomies (branches and endings) and assigns them a XY-coordinate that is then stored in a file.
Advantages:
- High correctness rate.
- Can execute 1-to-many judgements.
- Inexpensive apparatus.
- Easy to practice (samples are easy to imprisonment and reservation).
- Most documented and oldest of the biometric knowledge.

Disadvantages:
- Actual finger scan descriptions cannot be recreated commencing a stencil image.
- Users relate fingerprint credit to criminal action.

Face (or Facial) recognition: Face recognition is one of the original biometrics' technologies. The technology analyses facial characteristics and attempts to match it to database of digitized pictures. Face recognition uses distinguishing features of the face including the upper summaries of the eye socket, the parts adjacent the cheekbones, the edges of the mouth, to achieve verification and identification. The first step in the face acknowledgement is to obtain an image of a separate and stock it in a database for future expenditure.
There are four main methods actuality used for facial recognition:
- Eigenfaces: a tool established by MIT that excerpts characteristics over the practice of two-dimensional grayscale descriptions.
- Feature Examination (also recognized as Native)

Feature Analysis (LFA)): is the most lengthily used system because of its competence to neighborhood for facial changes and aspect. LFA uses a procedure to harvest a face print for judgement.
•**Neural network:** a technique that excerpts topographies from the expression and generate a pattern of contrasting rudiments that is then co-ordinated to a template in database.
•**Automated Face Processing (AFP):** a method that looks for reserves and ratios between persuaded facial landscapes, and is more perfect for out of sorts lit areas.
Advantages:
- High accuracy rate.
- Can be accomplished from a remoteness.
- Accepted by most users.
- Non-intrusive.
- Hands-free.

Disadvantages:
- Sensitive to lighting conditions.
- Can perform limited 1-to-many comparisons.

Iris recognition: No two irises are comparable, not even in one exact or in equal clones. The iris covers over 400 illustrious appearances. Therefore, iris scanning is greatly more exact than impressions or even DNA examination of the unique features. Iris scanning is performed by scanning the measures of the colored circle that surrounds the pupil.
In knowing one's Iris, there are two types of approaches that are cast-off by Iris documentation schemes, passive and dynamic. The active Iris system technique includes that a user be wherever from six to 14 inches gone from the camera. It also involves the user to move back and forth so that the camera can adjust and focus in on the user's iris. The passive system allows the user to be anywhere from one to three feet away from the camera(s) that locate and focus in on the iris.
Advantages:
- High accuracy rate
- Imitation is almost incredible

Disadvantages:
- perceived to be disturbing and invasive

- Can be completed from a short space
- Optical readers are problematic to work requiring progressive training for staffs

Hand geometry:

Hand geometry is troubled with measuring the corporal characteristics of the user's needle and digits and it is theoretical to be sufficiently unique for use as a means of biometric verification. The technology archives numerous sizes of the human hand, it is comparatively easy to use, and proposals a good equilibrium of performance characteristics.

RESULT

Application Areas:

The customs for biometric refuge are varied and rising. It remains. established in answer to a need to subordinate human action with identity whether conducting a deal, accessing a computer or a critical information system, or entering secure physical area.

Computer/Network security:

Many stand-alone and network computer systems convey appreciated and delicate information. Controlling access to these systems is another major use of biometric authentication system.

Internet transactions:

Due to growing security requirements that results from the boom in e-commerce, many thinks of on-line transactions as being an obvious area for biometrics. The biometric authentication produces a better degree of salesperson confidence because he knows that person that the person at the incurable is, he who he claims to be.

Physical area security:

Military, Government, and Commercial connections have satisfactorily strong confidentiality concerns.

Banking:

Several leading banks have been investigating with biometrics for an ATM use as a means of opposing card fraud. Beginning of 2002, some companies will be being delivering a smart credits card, with customer's fingerprint information embedded.

Voting: A logical use of biometrics is in voting process where qualified politicians are compulsory to verify their identity. This is projected to stop "proxy" voting.

Prisons: An interesting use of biometrics is in penitentiaries where the visitors to a prisoner are subjected to verification actions in order that identities may not be transacted during the visit.

Leading products in biometrics:

Biometric is a new but talented technology and therefore, a number of companies have seemed in the market in a less period of time. Some of those products are:

Security and Privacy

A nice property of biometric security systems is that security level is almost equal for all users in a system. This is not true for other security technologies. For instance, in an access control based on password, a hacker just needs to break only one password among those of all employees to gain access. In this case a weak password compromises the overall security of every system that user has access to. Thus, the entire system's security is only as good as the weakest password. This is especially important because good passwords are nonsense combinations of characters and letters, which are difficult to remember. Unfortunately, some users still use passwords such as "password", "Homer Simpson" or their own name.

Although biometrics offers a good set of advantages, it has not been immensely adopted yet. One of its foremost drawbacks is that biometric information is not secret and dismiss be replaced afterward being co-operated by a third gathering. For those submissions with a humanoid supervisor (such as boundary entrance switch), this can be a negligible problem, since the operator can pattern if the presented biometric trait is unique or fake. Though, for remote requests such as internet, some kind of energy detection and anti-replay occurrence devices

should be delivered. This is a developing research theme. As an overall rule, concerning security matters, a constant update is necessary in order to keep on being protected. A suitable system for the present time can become obsolete if it is not periodically improved. For this reason, nobody can claim that has a perfect security system, and even less that it will last forever. Another interesting topic is privacy, which is beyond the scope of this paper.

CONCLUSION

The advances in accurateness and serviceability and reducing cost have made the biometric technology a secure, reasonable and cost-effective way of identifying individuals. Biometric strictures such as fingerprint perusing, retinal the advances in accurateness and serviceability and reducing cost have made the biometric technology a secure, reasonable and cost-effective way of identifying individuals. Biometric strictures such as fingerprint perusing, retinal scanning, iris scanning, signature verification, hand geometry, voice verification and others are all well recognized with their own specific characteristics. The limiting factors of speed and band width are now a thing of the past and their practical performance might in many incidences be better than predictable.

FUTURE SCOPE

Exposure to a multi factor authentication method to include scanning of many biometric factors at once such as Google Abacus will also provide feedback on acceptance of cutting-edge biometric security. A comparison of answers prior to and after actual use of the device should provide insight as to the user's eventual comfort level with biometrics. Apple has embraced biometric security on the iPhone and may serve as a model for other companies and applications. The Touch ID on the iPhone is a fingerprint scanning authentication device first introduced in 2013. Theft of smartphones is a major problem especially in major cities, where it can account for up to 40% of reported crime. The widespread adoption of Touch ID has served as a deterrent to the theft of iPhones, since the fingerprint scan makes it so hard to access. "Given Apple's influence, the company's adoption of the fingerprint-scanner technology could increase the use of biometrics in identity verification and accelerate the demise of the password, which many feel has become outdated". Major online companies such as Amazon and Facebook need to strike a balance between making their sites easy to sign up with, using lax minimum requirements such as six-character passwords, versus requiring more security to protect their users. A biometric security option may be the solution.

REFERENCE

1. S. Furnell and K.L. Thomson, "Recognizing and Addressing 'Security Fatigue,'" Computer Fraud and Security.
2. Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 billion Units by 2020," Gartner, Inc., Gartner Press Release, www.gartner.com/newsroom/id/2636073
3. Biometrics for Secure Authentication", (PDF)Retrieved. Show Context Google Scholar
4. A. Jain, L. Hong and S. Pankanti, "Biometric Identification", Communications of the ACM, Show Context Access at ACM Google Scholar.
5. Available: http://www.biometricnewsportal.com/biometricsissues.asp.
6. Available: http://www.bioelectronix.com/what_is_biometrics.html.
7. Available: http://www.explainthatstuff.com/how-iris-scans-work.html.