IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 10-14
International Conference on Management Practices, Innovations & Research 2019

A Study about Security Essentials on Biometrics Authentication and Identification

Dr.M.Felix Xavier Muthu[1], Mrs.M.Angelin Rosy[2]

[1]Associate Professor, Mechanical Engineering, St.Xavier's Catholic College of Engineering, Anna University India

[1]Assistant Professor, MCA, Er.Perumal Manimekalai College of Engineering, Anna Universit,y India

Abstract: *Over the last few years a new area of engineering science It has been called "biometrics" to create a large market in the near future. The pioneers of this new domain intend to construct devices which would allows the identification of a person on the basis of their "biological" characteristics like voice, dynamics of movements, features of face recognition and other parts of the body, eye retina or iris pattern. Nature has been made the human beings with different kinds of characteristics which may vary from one person to another person. This is made of using Biometric technology to distinctly identifying each person. Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioral characteristic possessed by the users. Several most important issues must be considered in the designing a practical biometric system. First, a user must be entered in the system so that his biometric template can be captured and saved. This template is securely stored into a central database or in a smart card could be issued to the user. The template is retrieved when an individual needs to be identified during usage. Depending on the context, a biometric system can be operated either in verification (authentication) or an identification situation. Biometrics can be referred to the automatic identification of a person based on their physiological or behavioral characteristics.*

Keywords: *Biometrics, identity, characteristics, security, secret*

I. Introduction

Biometrics that allows a person to identify and authenticate, based on a set of recognize and verifying data, which are specific and unique to them. Biometric authentication is the process of comparing data for the person's characteristics to that person's biometric "template" in order to determine parity. The reference model was the first input in a database or a secure the portable element like a smart card. The data is stored and then compared to the person's biometric data to be authenticated. Here it has the person's identity which is being verified. Biometric identification consists of discovering the identity of a person. The goal is to capture an item of biometric data from this person. This can be a photo (image) of their face, a record (audio) of their voice, or an image of their fingerprint. This data is then compared to the biometric data of several other persons are kept in the databases.

II. Biometric Trends

Faced with identity theft and document fraud, with more new threats such as cybercrime or terrorism, and be faced with the understandable changes in the international regulations, new technological solutions are mostly being implemented. One of these technologies, biometrics, has been quickly established itself as the most pertinent means of identifying and authenticating with individuals in a fast and in the reliable way, through the usage of unique biological characteristics. Today, many applications were adapted for using this technology. That which in the past was reserved for the sensitive applications such as the security of the military sites is now developing rapidly through the more applications in the public domains.

III. Biometrics Information

Biometrics is the technical term for body measurements and calculations (scan). It refers to metrics related to the human characteristics. Biometrics authentication (or realistic authentication) was used in computer science as a meaning of identification and to be access the control. It is also used to identifying the individuals in groups that are been in under surveillance. If we were to define biometry or biometrics in the simplest sense, we would say the "measurement of the human body". There are two categories of biometric technologies.

III. Physiological Measurements

They can be either morphological or biological. Physiological measurements mainly consist of fingerprints, the shape of the hands, of the fingers, vein patterns, the eye (iris and retina), and the shape of the face (Human), for morphological analyses. For biological analyses mainly used measurements are the DNA, blood, saliva or urine may be used by the medical teams and for the police forensics.

In 2007 the Cogent Systems are recently acquired by the Gemalto. They began donating biometric software, hardware, and the support services for the university; leading to the creation of Cogent Systems Laboratory was located in the Oglebay Hall. The lab is equipped with a professional Automated Finger Identification System (AFIS), 24 workstations for finger/palm analysis, 3 live scans for enrolling prints, an Integrated Ballistics Identification System (IBIS), and a teaching station.

III. Behavioral Measurements

The most common behavioral measurements are voice recognition, signature dynamics (speed of movement of a pen, accelerations, pressure exerted, inclination), the way objects are used, keystroke dynamics, gait, the sound of the steps, gestures, etc. The different techniques are used to the subject of ongoing research and development, of course, and, are being constantly to be improved.

To see how the behavioral biometrics was gaining momentum in the Banking, visit our October 2017 web dossier. However, the different sorts of measurements all don't have the same level of reliability. Physiological measurements are usually considered to be offer the benefit of the remaining and more stable throughout the life of an individual. For example, they are not as subject to the effects of stress, in contrast to be identification by the behavioral measurement.

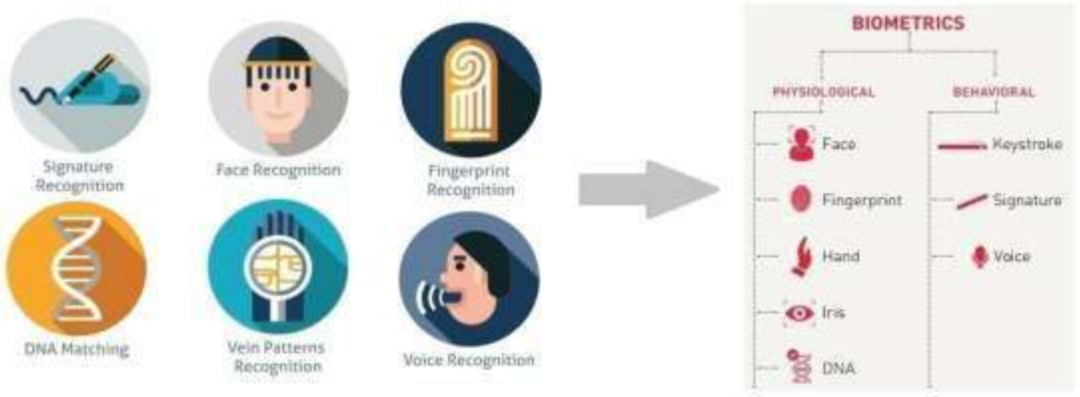

Fig: 1

Identity and biometrics

There are three possible ways to prove one's identity.

- It means of something that you can possess. Until now, this was something that was relatively easy to do and whether it was by using the key to one's vehicle, a document, a card, or a badge.
- By means of something that you know, a name, a secret or a password.
- By means of what you are, your fingerprint, your hand, your face.

The usage of biometrics has number of benefits. The leading one has the level of security and accuracy that it guarantees. Identities of biometrics are passwords, badges, or documents, biometric data cannot be forgotten, exchanged, or stolen, and cannot be forged.

The reliability of biometrics Authentication

Biometric authentication relies on statistical algorithms "false rejections" or "false acceptances". What's the story here?

- In one case, the machine fails to recognize an item of the biometric data that does however correspond to that person.
- In the reverse case, it assimilates two different items of biometric data that are not in fact from the same person.

Accurate of biometrics Authentication

The technical challenges of the automated recognition of individual identification based on their biological and behavioral characteristics are inherent into the transformation of analog (facial image, fingerprint, voice pattern...) to digital information (patterns, minutiae) that can be processed and compared or matched with the effective algorithms.

Fingerprints

There are about 30 specific points in a fingerprint scan obtained by the live fingerprint reader. The US Federal Bureau of Investigation (FBI) has evidenced that two individuals can have been more than 8 common minutiae. Recognition decisions in the biometric systems are have to be taken in a real time and, therefore, computing efficiency is the key in biometric apps. It was not the case in biometric forensics where the real-time recognition is not to be a requirement.

Facial Recognition

Facial recognition is one of the most natural means of a biometric identification. The face recognition system does not be required any contact with the person. The 1000 million electronic passports in the circulation in mid 2017 provide a huge opportunity to the implement face recognition at the international borders. Guidelines to improve the quality of the reference picture embedded in the e-passport micro-chip are provided by the ISO/IEC 19794-5 standard and used by the International Civil Aviation Organization 9303 standard for passport photographs.

Tokens and biometric ID cards

Biometrics can suffers from the fact of the matching algorithms cannot be compared to the hashes of the passwords, as we said. This means that the two biometric measures are cannot be compared with the each other without them, at some of the point, being "in plaintext" in the memory of the device was doing the matching. Biometric checks must therefore be carried out on a trusted device, which means the alternatives are to have a centralized and supervised server, a trusted terminal, or a personal security component.

Smart ID cards

This is why the tokens and smart cards (IDs or banking cards now) are increasingly are been used as the ideal companions for a biometric systems.

Fig : 2

Numerous of national identity cards (Portugal, Ecuador, South Africa, Mongolia, Algeria, etc.) are now incorporate in the digital security features, which all are based on the "Match-on-Card" fingerprint matching algorithm. Unlike the conventional biometric processes are, the "Match-on-Card" algorithm will allows fingerprints to be matched locally with a reference of frame thanks to a microprocessor to be built into the biometric ID card and it be without having to connect to a central biometric database.

Biometric sensor cards

Another form of the delivering a safe and the convenient way to authenticate with people has been enabled with the integration of a fingerprint scanner into the smart cards.

Fig : 2

These biometric sensor cards are open up a new dimension in the identification with an easy-to-use, portable and a secure device. They are been launched in the year of 2018 for the first time by Bank of Cyprus and Gemalto for EMV contactless and the contact payment. They can be use the fingerprint recognition instead of a PIN code to authenticate with the cardholder.

Biometrics and data protection

While there are hardly to any legal provisions in the world that are specific to the biometric data, can despite the very specific character of such data, the French Data Protection Act of 1978, officially entitled as the "Loi relative à l'informatique, aux fichiers et aux libertés " [English title: Act on the Information Technology, Data Files and Civil Liberties] sets out the specific requirements for the biometric data.

The "United Nations Resolution" of December 14, 1990, which sets out the guidelines for the regulation of a computerized personal data files, It does not have any binding force. On the contrary, the new EU regulation replaces the existing national laws as of May 2018.On a more global basis, legal deliberations thus rely to a very large extent on the provisions are relating to the personal data in the broad sense. But such of the provisions are sometimes proving to be poorly adapted to the biometrics.

Putting biometrics to work for digital security

Gemalto possesses its own technology, to be recognized in worldwide, which, combined with its impartial stance on the source of the biometric data, and it allows to help everyone can put their trust in the digital world. An expert in the strong identification with more than 200 civil ID, population registration and the law enforcement of projects that can incorporate biometrics, Gemalto is able to act as an independent force in the proposing and to be recommending the most suitable solution in each case.

Gemalto attaches a great deal of an importance to the assessment of risks are which may not always to be visible to the general public, and to the capacity of the private operators that can manage such risks. Similarly, the legal and social implications are also been very important. Though Gemalto keeps an open mind and with regard to the biometric techniques, it remains with no less convinced that, whatever these choices of biometric, this technology will offers major benefits for the guaranteeing identity.

VII. Conclusion

Biometrics is the automated recognition of an individual is based on their behavioral and biological characteristics. It is a tool for establishing the confidence and that one is dealing with the individuals who are already known (or not known) and consequently that they can belong to a group with a certain rights (or to a group to be denied certain privileges). It relies on the presumption of that individuals are physically and behaviorally distinctive in a number of ways.

Biometric systems are been used as increasingly to recognize the individuals and regulate the access to physical spaces, information, services, and to the other rights or benefits, including the ability to cross the international borders. The motivations for using the biometrics are diverse and often to a overlap. They can include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing the public safety and the national security.

References

[1]. Ms. Shraddha S. Giradkar, Dr.N.K.Choudhari, A survey paper on Various biometric security system methods, International Research Journal of Engineering and Technology, Volume: 03, Issue: 02 | Feb 2016 (IRJET), e ISSN: 2395 0056

[2]. Esther Rani.D , Dr. J. John Raybin Jose, fingerprint based biometric authentication, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September-2016, pg. 6-15, ISSN 2320 – 088X

[3]. Krishna Dharavath1, F. A. Talukdar2, R. H. Laskar3, Study on Biometric Authentication Systems, Challenges and Future Trends: A Review , IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[4]. Elena Pagnin and Aikaterini Mitrokotsa, Review Article Privacy-Preserving Biometric Authentication: Challenges and Directions,Published 19 October 2017

[5]. Abhilash Kumar Sharma, Ashish Raghuwanshi, Vijay Kumar Sharma, Biometric System- A Review, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4616-4619, ISSN NO : 0975 -9646