Research Article Impact Factor: 4.226 ISSN: 2319-507X
Parikshit R. Deshmukh, IJPRET, 2015; Volume 3 (9): 1481-1488 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

THE ADVANCE AUTHENTICATION SYSTEM – BIOMETRICS ITS FUTURE APPLICATION AREAS

PARIKSHIT R. DESHMUKH[1], PROF. NITESH M. TARBANI[2]

1. Student of Master of Engineering in (CSE), PRMIT&R college of Engineering and Technology, Amravati, India.
2. Assistant professor Department of (CSE), PRMIT&R College of Engineering and Technology, Amravati, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Biometrics are an important and widely used method for identifying proper person to control access for providing security in today's growing computing world. A biometrics does this by using physiological and/or behavioral characteristic used for automated recognition of an individual from his physical and behavioral characteristics, which is mostly unique. This system recognize many individual's biometric characteristics, such as fingerprint, hand geometry, DNA, ECG and Voice, signature, walking behaviors, and many others. It has large amount of application in physical assets like laboratories, hospitals, and banking from ATMs and online. It also used to determine whether a person is in a database for enrollment verification, or national ID applications, the process of verification is studied in this paper. As there is growing need of authentication we are presenting the future application areas of this efficient validation technique which makes our living standard better, fast and secure.

Keywords: Biometrics, Physical biometrics, behavioral biometrics, Biometric recognition, Access control, Travel control, Remote Authorization.

Corresponding Author: MR. PARIKSHIT R. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Parikshit R. Deshmukh, IJPRET, 2015; Volume 3 (9): 1481-1488

PAPER-QR CODE

INTRODUCTION

Biometric refers to the method of recognizing a person based on physiological or behavioral characteristics. Biometric technologies are becoming an additional layer of authentication added to existing system based on the current computing environment. It becomes todays need for robust system, encountering the security breaches and transaction frauds. This technology caught the attention of major IT vendors and it is regarded as an area that no segment of the IT industry can afford to ignore. Biometrics provides a hierarchical structure of data protection, making the data more secure. Biometrics refers to metrics related to human characteristics both physical and behaviors, for authentication and access control is widely used in many computer science applications [1].

All of the measures used for authentication mainly contains both physiological and behavioral components of the person, both of these components can vary among all people similarity is very rare situation [2]. Biometrics system is act as the use of computers to recognize people, for various activates as in the field of E-commerce developers are exploring the use of biometrics and smart cards for accurately verify a trading party's identity. Banks are bound to use this for better authenticate customers and ensure non-repudiation of online banking, trading and purchasing transactions. It can helps to obtain secure services over the telephone through voice authentication. Researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas like airports. Biometrics is being used to improve mainly for identity verification and access authorization, passenger identity verification, and flight crew identity verification. Which protect against unauthorized access using lost, stolen, or forged badges.

In this paper we are giving some additional functionalities which gives better securities and trust for identity verification as remote authorization, Financial and other transactions requiring authorization, Travel control, Authentication and attendance monitoring, etc. This will help rare and critical attack like**,** a terrorist on watch list attempting to obtain a credential using an assumed identity; and impersonation of a pilot, air traffic controller. Although there are legal concerns about civil liberties with overly intrusive security systems, utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods of utilization of passwords or PINs. The need of the hour is a technology to replace the inefficient current system that relies on manual workers handling critical machines. Therefore, Biometrics is the technology that the future will hold, although there are still considerable political and airline resistance that needs to be tackle by giving remote authorization method.

Technologists are constantly working visualizing the next generation security systems for multimodal biometrics, aliveness detection, gait analysis etc [3].In addition, researches are in progress to minimize the manual intervention of the user with the system to give proper assurance. This paper will explain the biometrics technologies its functional working and the potential market demands projected by the research reports in different modalities of biometrics and application areas. As biometrics refers to metrics related to human characteristics for authentication and access control the distinctive, measurable characteristics of multiple sensors or biometrics identifiers are used to label and describe individuals. Access control include for token-based identification systems, such as a driver's license or passport. For an individuals, biometrics are more reliable in verifying identity than token and knowledge-based methods; But in addition to this positive secure side, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [4].

Biometrics are among the most advanced and valuable security technologies available. Devices that scan facial features, irises, fingerprints and other physical characteristics have secured some of the most sensitive facilities in the world for many years. This techniques being used for more routine purposes of authorization, from controlling access at different department and to verifying identities for financial transactions and accessing different features at the need of advancing and fast developing areas of life to make all the work remotely and quickly.

II. FUNCTIONAL WORKING OF BIOMETRIC SYSTEM

The operation of Biometric systems components mainly involves two phases, namely enrolment and recognition [6, 7]. Both phases involves the use of biometric sensors such as cameras, microphones, fingerprint scanners, and tablets. The specific biometric human traits from individuals and convert to capture the input samples into relevant digital format, and the salient features are extracted into biometric templates. An optional pre-processing module may exist in two processes; particularly clean the samples which may be subjected to various types of noise and interference, and to prepare the samples into appropriate format for feature extraction. The biometric templates are then stored in the databases as individuals references.

Biometric recognition often makes use of a comparator module which can be carried out in two different modes that are user verification and user identification [6, 7]. The user verification performs authentication based on `are you person who is claiming?' mode. This mainly involves a straight forward comparison of one-to-one basis, whereby the final verdict is a binary i.e. `accept' or `reject' decision. The identifiers are usually in the form of user IDs or smartcards. On the other hand, the user identification performs an exhaustive one-to-many searches on the

entire user database to solve the `who are you?' question. Figure 1 below illustrates the components of a biometric system.

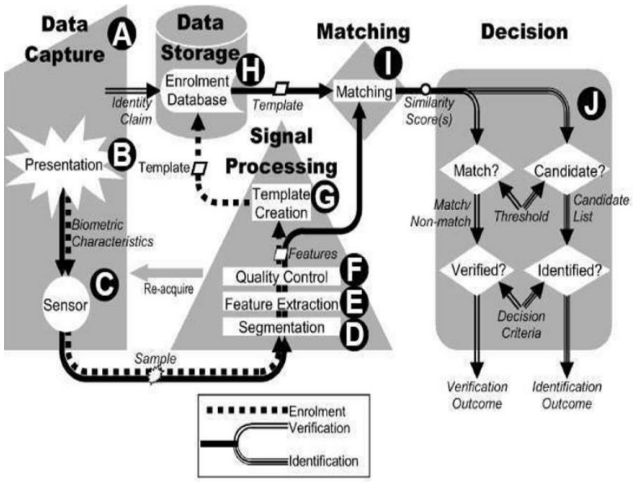

Fig. 1. Block diagram of a components biometric authentication system [8]

To better understand security issues concerned with biometric authentication, it should be useful to study individual components of a biometric authentication system and communication channel among the components, and their vulnerabilities. Figure1 [8] shows major functional components of this system, where major steps in the process of authentication is marked alphabetically as A, B,C, and so on. Each presented sample (B) is acquired by a sensor (C) processed via segmentation and feature extraction (D) algorithms. If available, a sample quality assessment (E) algorithm is used to indicate a need to reacquire the sample. Biometric features are encoded into template, which is stored (H) in database or any secure hardware. In the biometric encryption systems, a code or token is combined with the biometric feature in the template. At the time of enrollment, biometric samples are linked to a claimed identity (A), and during subsequent verification or identification, samples are compared with enrolled samples using matching algorithm (I), and an identity decision (J) is made automatically, or by a human being reviewing biometric system outputs [5].

III. FUTURE APPLICATION AREAS OF BIOMETRICS

A. Access and attendance control

In the near future, biometrics will certainly gain increased acceptance in access and attendance control applications of all kinds. It is expected that, biometrics will be used for these applications in homes, offices, computers, machines, devices, etc, which create largest market

for biometric technology [9]. Secondly, the use of these devices will be for replacing existing access control methods and technologies, which provides increased convenience and security. This reduce our tasks for carrying keys, identity cards, personal documents, etc. Furthermore, this implementation of biometrics for overall security solution: for the possibility of theft or unauthorized use of equipment/technologies.

B. Travel control

At the time of people traveling via planes, ferries, and even trains to be individually registered, there are checks perform at multiple locations. Today it becomes an increase requirement mostly by security concerns, visa regulations and other such reasons. As, the amount of people traveling is already large and increasing day-by-day at significant rates, all organizations involved in transportation industries are very interested in the automation of necessary procedures. For example, especially in the case of International Civil Aviation Organization. This is trying to introduce biometric passports, visas and other controls/documents. This organization recommends clearly, that Contracting States should incorporate biometric data in their machine-readable passports, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine-readable zone.

C. Financial and other transactions requiring authorization

Today the applications having to do with money this happens in form of credit or bankcards, pocket electronic money, etc. However, it is clear that, in most cases, the physical card is not important, because money has an owner that can bedirectly connected to a person. Spreading of biometric authentication in the economic sector mostly in banking and trade will replacing the need for physical objects, such as cards with the use of virtual money. This will result in a significant change for both general people and financial organizations. The possibility to authorize all legal transactions through biometric mechanisms will make many of these operations much easier and more convenient.

D. Remote authorization

By merging existing and future networking developments along with biometric solutions will allow people to have the opportunity to authorize a wide range of transactions mostly for voting, purchasing, accessing, decision-making authorizations, etc.It is no longer needed to personally present at a given location in order to authenticate a specific action [9]. This action seems possible today but it is also true that remote authorization on a large scale, such as public elections, will not be realistic until appropriate biometric solutions are operating for

particular solutions. For this, it will be necessary to develop new, more robust and capable devices. Such devices can also be used for other places as computers accessories, access control devices, etc. However, after more accurate, reliable and cost-effective devices are developed that are not constrained to shortcomings associated with existing technologies, the potential for authenticating remote transactions, such as for voting can drive major changes in all democratic societies as the idea for direct democratic participation by the public can be realized on a large scale and at low cost.

Necessary democratic decisions can be made practically every day at minimal cost, even in large societies. The possibility of low cost remote voting by the public will not only open up the potential for increase participation, but also for increased frequency in voting activities. It is only speculation today, but I would think that this perspective can lead to some of the largest changes in democratic societies – all facilitated by the introduction of accurate, reliable, high speed biometric technologies that enable remote authentication (voting, et al.) at minimal cost. The corresponding changes in political systems and power structures will provide the potential to have a more representative democracy in all the democratic nation.

In association with remote voting and authorization it also influence economy and tax system: the control of money transfers will be easier, and also compete within the “black economy”. To authorize any transaction remotely will surely cause additional changes in other transactions that will have impact on life in the near future which will minimize, or eliminate the need for personal contacts. Such operations will be easier and can be done automatically.

E. Use of automatic working devices

With biometrics, it will be easier to track the actions of user for any devices and machines, for adapting their functions to his needs and to demand his liability for actions caused. This feature will change many areas of life and create a large market for devices that are able to recognize their users and react according to their needs. The main goal of this development is to create the machines able to recognize their user or people doing something in their vicinity. For example, this feature can be very important or convenient in factories, offices, hospitals, for use of cars, home appliances, etc. The machine “knows” who is using it, which allows automatic adaptation to the needs of people, but also tracking of their actions and reacting in the case of misuse.

These kind of biometric functions do not require a very high degree of secure recognition, but will require multimodal biometrics techniques like face, voice, gait and habits recognition and probably much more. Today such functions will be implemented in many devices, because of

the convenience, that they are offering. In industrial environment the importance of their use will grow, offering significant advantages, quicker reaction to the user for example in the form of establishing the environment that suits to the person and actual using the device. This offers a convenience and a time gain adjusting such functions requires some time that must not be lost [8]. The machine could do this automatically. It allows also implementing such functions for correction of specific errors, made by the user and use of shortcuts that can be adjusted individually. Broad use of such technologies also support the development of automatic shops and facilities operated without employees. The many machines will be able to recognize the needs of their users automatically, becoming more and more able to serve people in the similar way as live servants.

F. Action control

The last facility, for the market that can be seen as a part of previous ones but it has special features and can require specific devices. For the case of potentially dangerous devices, it is necessary for good control and the use of them that prevents unauthorized people can use them or to track, who has used them in a specific situation. This can be used with cars, that should not be used by people without driving license or drunken, with dangerous machines, that must be used by people only having appropriate knowledge and a special case of weapons. It would be very good if only authorized person could use every critical devices [9]. This would make the use of plundered weapons impossible, and allow to track, who has used a specific weapon for a crime. This market is specific, because biometric devices for action control must have special features. In the case of real time requirement, this biometric for authorized person is most important for proper validations. In practically all cases, they must be integrated in handles, triggers, steering wheels, etc. In some cases, they must also be able to recognize the condition of the user and eliminate for example drunken car drivers.

IV. CONCLUSION

In summary, biometrics technology is most important technology for most of us implementing in public and advance sectors. This biometric system is mostly used for authentication system in today's modern world. Biometric has characteristics mainly based on physical and behavioral parts and function of the body. This paper presents functional working of this biometric security system, which improve our lives with improved security and effectiveness, reducing fraud, and costs for authentication. In this paper, we are giving some of the future application enhancements that makes it easy to use and makes live consisting of some daily concern more comfortable along with some disadvantages caused in some sectors overcome. Even though

the biometrics authentication system still has many concerns such as information privacy, physical privacy so it is necessary to provide solution for security concern so that we will make our living standard more better in today's computing and advanced world with the given advance facilities in different sectors provided by biometric.

REFERENCES

1. "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Retrieved 2012-06-10.

2. Ashraf El-Sisi, "Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filtere", The International Arab Journal of Information Technology, Vol. 8, No. 4, October 2011.

3. THE CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES [Online] available: http://fas.org/irp/congress/2013_hr/biometric.pdf.

4. Jain, A., Hong, L., &Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110.

5. James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric Authentication Systems" Springer Journal, (Eds) 2005.

6. K. A. Rhodes, Information Security: Challenges in Using Biometrics, United States General Accounting Office, 2003.

7. S. Prabhakar, S. Pankanti and A. K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security and Privacy, vol.1, no.2, pp.33-42, 2003.

8. A. Adler. Biometric System Security. Springer, US, 2007.

9. Future of biometrics [Online] available: http://www.optel.pl/article/future%20of%20biometrics.pdf.