International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 013-017
e-ISSN:2278-621X

AN ANALYSIS OF MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM IN DIFFERENT AREAS FOR PROPER NETWORK SECURITY

A Kavitha[1] & A Vanaja[2]

Abstract-In todays the world is fully covered with latest technologies. Consequently the privacy is still in big issue. In earlier days traditional authentication methods like passwords, PIN and identity documents are inadequate to ensure security due to lot of drawbacks in this system now a day's most of the area use biometric for reliable and secure authentication. Biometric provides high security with more accuracy which identifies the person based on their physiological or behavioral characteristics of a human being by using biometrics technology. This paper gives a review of the areas where the biometrics has been used. It concludes that the biometric will increase security, reliability and acceptability in the latest technology of computer system. Future trends in biometric technologies are also discussed.
Keywords: Network Security, Authentication, Multimodal Biometric.

1. INTRODUCTION

Information security is the process of securing the data from unauthorized access and ensure that only the valid person can able to access the data in the server. Because of the owner of the content such as authorized person, authorized distributors are losing the most data due to copying and sharing the data. Secure technologies like digital certificates, digital signatures, and data encryption services to protect the data from being accessed by unauthorized persons. In order to solve this problem lot of security systems are introduced to protect the data.

The security field uses three different types of authentication:
1. Something you know - password, PIN, or personal information
2. Something you have - card key, smart card, or Secured card
3. Something you are - a biometric.

A biometric authentication is new technique with high reliable and secure authentication tool among the three fields. It can't be easily stolen, forgotten or duplicated and forging by any one is impossible because physical characteristics of every human are unique. It much more difficult to attack then security codes, passwords. Biometric technology plays a major role in personal authentication for large scale enterprise network authentication environments.
Biometric classified as two types such as unimodal and multimodal. Unimodal biometric systems use only one biometric trait (fingerprint, face, iris, retina, voice etc.) to recognize individual. It has some limitations over authentication like noise in sensed data, intra-class variation, inter-class variations, spoof attacks etc. Therefore unimodal biometric system is less secure and less reliable and the usage of this system become less where high security required. It can be overcome by multimodal biometric system which incorporating multiple traits of individuals rather than one trait. An accurate identification or authentication system can be implemented using various biometric traits of a person such as fingerprint, face, iris, palm print, signature etc. The following fig1 shows the different types of biometrics.

[1] Research Scholar, Chikkana Government College of Arts & Science, Tiruppur
[2] Research Scholar, Visvesvaraya Technological university, Belagavi, Karnataka, India

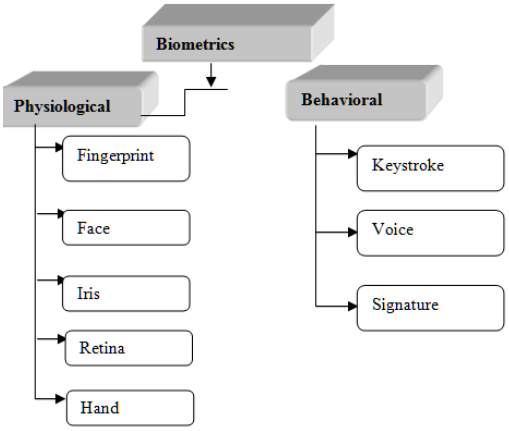


Fig1: Types of Biometric system

2. FUNDAMENTALS OF BIOMETRIC

Generally Biometric system can be defined as the automated process of identifying or authenticating the human being based on the human physical or behavioral characteristics and can either be identification or authentication system.

2.1 Identification

The sample template is compared with the entire database of trained biometric samples. This type of process is called as one-to - many processes.

2.2 Verification

The sample template is tested with the claimed biometric samples in the database. This type of process is called one - to - one process.

The biometric authentication system is a two-stage processes namely the enrollment and the authentication. Each step involves following three sub-stages: Biometric sample capture, Pre-Processing and Process into a reference template and Compare processed input sample against reference template in database.

2.3 The Enrolment or Registration stage

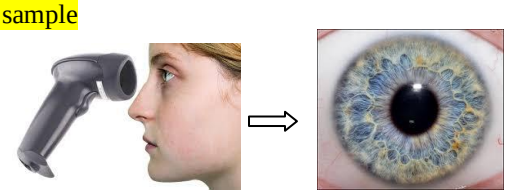
During this stage, each person is supposed to register his biometric trait into the database which is done by the biometric sensor that it captures a sample of biometric trait of a person. Captured biometric sample is pre-processed and processed into a template and it is compared against the stored biometric sample templates.

2.4 The Authentication Stage

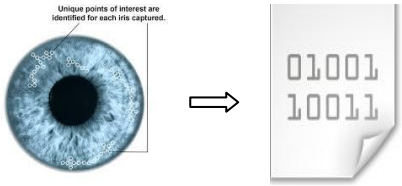
Authentication process is similar to enrolment stage except the difference in matching stage. Unlike in enrollment stage, the person will be authenticated for the authorized service only if a match of the input biometric sample is found against the stored biometric samples in the database. The person will be rejected otherwise. The following fig2 shows the process of person identification.

Multimodal biometric system fuse the information obtained from different sources to overcome some limitations of unimodal biometric systems. The key to success of multimodal biometric system is in an effective fusion scheme, which is necessary to combine the information presented by multiple sources. This is done to improve the accuracy, efficiency, and robustness of biometric systems.

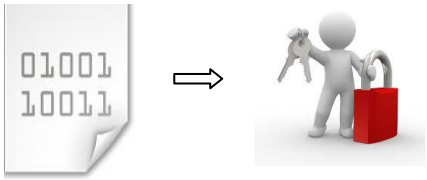
1. A biometric sensor is used to produce a sample



2. An algorithm extracts the sample's most characteristic feature which are used to produce template



3. At Enrollment template is saved in secure storage



4. At verification a fresh template and the enrolled template are compared by an algorithm and to decide whether it was a match or a nonmatch

Fig 2: Key steps for Unimodal identification system

3. APPLICATIONS OF BIOMETRICS

Biometric authentication can be incorporated in a wide range of sectors they are,

3.1 Banking and Financial

The internet has grown to greater high in the banking and financial field. Consumer may use lot of benefits through online shopping. Identifying intruders in this field is still in critical process. Incorporating biometric in this field provides a greater security to online banking and customer financial information.

3.2 E-commerce

E-commerce developers are mostly preferred biometric based smart card for the business process. It reduces the fraudulent by 90 percent.

3.3 Healthcare

In this field biometric are mostly used to keep the patient records confidentially.

3.4 Time and Attendance

Business, industry and corporate used biometric based attendance system (fingerprint recognition, Face recognition etc) to ensure the employees attendance.

4. LITERATURE REVIEW

Maria De Marsicoe et al [1] developed FIRME (Face and Iris recognition for Mobile Engagement) as a biometric application based on a multimodal recognition of face and iris which was implemented as an embedded application for mobile devices using Android with high security. Score level fusion was applied to fuse the two biometric modalities.

Esteban Vazquez-Fernandez, Daniel Gonzalez-Jimenez [2] proposed a biometric system as Face recognition for authentication on mobile devices which provides usability, security, robustness against spoofing attacks, and user privacy among others.

Shengrong Bu [3] et al developed Intrusion Detection system in High-security Mobile Ad Hoc Networks with the help of ultimodal biometric technology.

Weizhi Meng et al [4] surveyed around 243 users on development of biometric user authentication techniques on mobile phones, especially touch enabled phones, according to physiological and behavioral characteristics and identified physiological biometrics can provide high authentication accuracy.

Donny Jacob Ohana et al [5] introduced biometric authentication system for identify theft and intrusion detection on mobile phones.

D. RAMESH et al [6] introduced highly secured railway reservation system using biometric technology. It simplifies the reservation system in that fingerprint of the person who goes for reservation/ticket booking and it verifies the person with previously stored data using standalone module as a part of verification.

Dhvani Shah, Vinayak Bharadi [7] proposed a IOT based biometric architecture on Raspberry Pi. The encrypted biometric trait was sent from RPi client to the Azure cloud for decryption. The proposed system can be used for security and access control mechanisms like unlocking a door, logging details of a person, attendance management, accessing a particular service etc. It can be applied at all places where authentication is required.

Cristian Morosan [8] surveyed on biometric E-gates in airports for secure air travel system. It allow security agencies to allocate their resources efficiently while making travel more fluid in sensitive areas of airports

Nana Kwame Gyamfi [9] et al identified a model for the modification of existing ATM systems to incorporate fingerprint scanning and, outlines the advantages of biometric ATM system.

Ankit Kumar [10] focused on various security approaches of ATM and stated that Biometric Authentication with Aadhar cards With OTP Password is a stronger method of authentication and verification as it is uniquely bound to individuals.

Ms. Swati S Bobde, Prof. D. N. Satange [11] concluded that the multibiometrics can be embedded in mobile phone which provides high secure E-Transaction.

Sakthivel .A, Jayakeerthi [12] proposed a multi-biometric model(integrating voice, fingerprint and facial scanning) that can be embedded in a mobile phone which made transactions more secure.

Kirat Pal Singh [13] proposed a new approach to network security based on contactless palm vein biometric system. It provides more security with less key length and there is no need to store any private key anywhere.

O. A. Esan, S.M. Ngwira and T. Zuva [14] developed a bimodal authentication system (fingerprint and face) to protect the patient's medical record on PC.

5. CONCLUSION

Biometrics is an essential component of any identity-based security system because no other technology can replace the requisite functionality of "identifying the authorized person based on their intrinsic distinctive traits." Achieving security through biometric has been done in lot of areas successfully. Biometrics are widely used in many type of network (WSN, MANET etc) for providing high security. The future work will be incorporating biometric for enhance the security of MANET.

6. REFERENCES

[1] Maria De Marsico, Chiara Galdi , Michele Nappib, Daniel Riccio "FIRME: Face and Iris Recognition for Mobile Engagement", Elsevier, Image and Vision Computing 32 (2014) 1161–1172.

[2] Esteban Vazquez-Fernandez, Daniel "Face recognition for authentication on mobile devices", Elsevier, Image and Vision Computing 55 (2016) 31–33.

[3] Shengrong Bu, F. Richard Yu, et al "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, NO. 3, MARCH 2011

[4] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones", IEEE Communication Surveys & Tutorials, Vol. 17, No. 3, Third Quarter 2015

[5] Donny Jacob Ohana ,Liza Phillips, Lei Chen," Preventing Cell Phone Intrusion and Theft using Biometrics", 2013 IEEE Security and Privacy Workshops

[6] D. Ramesh, B. Kantha Rao, Ch. Meena Kumari," Highly Secured Railway reservation using Biometric Technology",International journal of scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04,Issue.17, June-2015, Pages:3130-3135.

[7] Dhvani Shah, Vinayak Bharad,"IoT based Biometrics Implementation on Raspberry Pi",ELSEVIER, 7th International Conference on Communication, Computing and Virtualization 2016, 328 – 336.

[8] Cristian Morosan," An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports", ELSEVIER, Journal of Air Transport Management 55 (2016) 120 – 128.

[9] Mustapha Adamu Mohammed, Nana Kwame Gyamfi, Dr. Ferdinand Katsriku," Enhancing the Security Features of Automated Teller Machines (ATMs): AGhanaian Perspective", International Journal of Applied Science and Technology Vol. 6, No. 1; February 2016.

[10] Ankit Kumar ,"A Review Paper On ATM Machine Security With BIOMETRIC OR Aadhar Card and OTP Password", 4thInternational Conference on System Modeling & Advancement in Research Trends (SMART) College of Computing Sciences and Information Technology (CCSIT) ,Teerthanker Mahaveer University , Moradabad,2015.

[11] Ms. Swati S Bobde, Prof. D. N. Satange," Biometrics in Secure e-Transaction", International Journal of Emerging Trends & Technology in Computer Science,Volume 2, Issue 2, March – April 2013 ISSN 2278-6856.

[12] Sakthivel .A, Jayakeerthi .M," Secure E-Transactions through Bio Metrics System", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358

[13] Kirat Pal Singh," Biometric based Network Security using MIPS Cryptography Processor", Proc. of QSHINE'13, LNICST Springer Link [12]

[14] O. A. Esan, S.M. Ngwira and T. Zuva,"Bimodal Biometrics for Health Care Infrastructure Security" Proceedings of the International MultiConference of Engineers and Computer Scientists 2014 Vol I, 2014, March 12 - 14, 2014.