I J C T A, 9(17) 2016, pp. 8615-8622
© International Science Press

Performance Analysis of Biometric Technologies Based on Identified Significant Metrics for Deployment in E-banking

Munish Sabharwal

ABSTRACT

The study was carried out with the aim to conduct performance analysis for the different biometric technologies presently available based on the significant metrics for biometrics deployment in E-Banking. The study is pursued by assimilating information through a literature review for identifying the various types of biometric technologies presently available as well as to identify the significant metrics affecting their performance based on the analysis of the concerns, opinions and perceptions of bankers, customers and technologists for deployment of biometrics in e-banking.

Conclusively a performance analysis is conducted on the identified biometric technologies based on the identified combined significant metrics.

The study puts forward the summary of performance analysis for the various biometric technologies presently available based on the combined identified significant metrics for deployment of biometrics in e-banking and in addition recommends the biometric technologies that are presently the most suitable for deployment in e-banking.

Keywords: E-Banking, Biometric Technologies, Biometrics Deployment, Significant Metrics for Biometrics Implementation, Performance Analysis

I. INTRODUCTION

The commerce is increasingly relying on the e-commerce model and with the increase in internet based trade there has been a corresponding increase in the online frauds, specifically in e-banking and e-business channels.

According to Munish, the core of today‘s business is Information and the all-encompassing influence of IT in harnessing, collating and processing huge volumes of information is ultimate. In such scenario it is essential to ensure the confidentiality of information while adhering to accepted norms of privacy and making it accessible to legitimate users at the suitable time assumes great importance. This scenario essentially implies more aptly for the banking sector in which day-to-day operations are centred on information and information processing, which themselves are highly Technology dependent [1].

Privacy as well as security of systems and installations has always been imperative and exigent but they have become more central in this age of e-business, where it is regarding the security as well as privacy of data in electronic mode. In the contemporary society personal identification or authentication has a very critical role as it facilitates in enhancing the security by the identification of a person.

Passwords or PIN (Personal Identification Number) are extensively used by IT based systems to verify a user to a system but the identification of a Password or PIN does not mean the detection of the person's identity since access to a PIN, a Password, a card or any other 'key' that is being used to get access to a

[*] Executive Director and Professor (School of Engineering and Technology), KITE Group of Institutions, Meerut, (U.P.), INDIA, *E-mail: mscheckmail@yahoo.com*

device can be gained by anybody fraudulently. This means that systems that are dependent on high access security cannot always rely on these kinds of tokens, since they cannot ensure that a user is who s/he claims to be.

In today’s technology and gadget intensive world, an individual has to remember passwords for net banking, personal and professional emails, government and organizational login, social networking sites, Mobile Banking, Cloud Storages, E-Stores and other related sites, with the need to remembering one additional password virtually every few days. Remembering all such passwords is getting increasingly cumbersome and difficult as well forgetting them involves hassles and disclosure or leak may prove to be fatal. Therefore a novel, convenient as well as secure technology is required for authentication as well as transaction operation.

In order to cover the limitations associated with the conventional methods of authentication, an authentication mechanism-based on what you are (biometrics) was initiated. Instead of traditional methods like PIN’s or passwords, biometrics could be used to gain trust to a device. The biometrics based authentication mechanism can be used to prevent access to restricted areas and installations as well as critical information.

Edmund Spinella describes that the word “biometrics” comes from the Greek language and is derived from the words bio (life) and metric (to measure). In his study Edmund refers to biometrics as the technologies used to measure and analyze personal characteristics, both physiological and behavioral. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft, more and more organizations are considering biometrics a solution to their security problems[2].

Any Biometric system operation includes the following: Enrollment-(measuring and storing of the physical or behavioral characteristics of user), Utilization – (that is the use of a biometrics system by a user through his individual physical or behavioral biometric characteristics for authentication), Update-(that is updation of the physical and behavioral biometric data of the user after a prolonged duration as there may be some change in the individual biometric characteristics with time).

There has been a significant escalation in the use of biometrics for user authentication in recent years because biometrics-based authentication presents several advantages over other authentication methods. Traditional authentication mechanisms are inferior to biometric authentication mechanisms like passwords/ PIN’s as they can be guessed, forgotten, copied, stolen, misplaced etc where as biometrics ensures the secrecy of personal information and provides a high degree of security and convenience as it uses distinct biological / behavioral characteristics of an individual which are inseparable from him, consequently reducing the danger of loss or theft. Biometric technology aids in preventing theft as the information is stored in the form of a digital record in the database which makes it highly improbable to recreate, maneuver and decrypt.

There have been several studies in the recent past that suggest that biometrics has can be fairly successfully implemented in various channels of e-banking and in addition it enhances the security of the existing system. Wayman and Maio suggest that the declining costs of the sensors and growing reliability of the associated software used to enroll and compare fingerprints has resulted in an increasing number of cost-effective commercial systems being deployed to verify customers at point of sale (POS) terminals. Other important areas of application of this method of authentication in the banking industry are the ubiquitous automatic teller machines (ATMs) and Money Access Centre’s (MACs)[3]. Prof. Selina Oko in her study improves the existing security of the ATM (Automated Teller Machine) system by integrating the fingerprint of the user into the bank's database as to further authenticate it. This was achieved by modeling and building an ATM simulator that will mimic a typical ATM system [4].S.T. Bhosale & Dr. B.S.Sawant in their study deals with new innovative model for biometric ATMs for the rural farmers, semi-literate people, which replace card system by biometric technology for operating ATMs. Proposed model provides high security in authentication which also protects service user from unauthorized access. In this proposed model user required to authenticate himself with biometric identification (Thumb/ Fingerprint/Iris etc.), Personal Identity Number (PIN) and selection of bank branch from displayed list if necessary[5].

There have also been several successful implementations of biometrics in various channels of e-banking. The Hindu for instance reported that Chinese researchers have successfully developed the first automated teller machine (ATM) with facial recognition technology to reduce the risk of theft [6]. The use of biometrics like Finger Print, Face and Iris recognition in smart phones is increasing becoming common feature and Angela Sasse for **www.theguardian.com** reports that people are fed up with battling to remember dozens of passwords. Entering them several times a day on various devices disrupts users' flow and wastes time. Employers and service providers have started to realize this and are offering alternatives in the form of sensors and biometrics. Fingerprint biometrics have been available on mobile phones for a while, but the addition of Apple's Touch ID marks a point of no return in the second coming of biometrics. While some security experts may be concerned about the use of fingerprints on their own, for customers it is a welcome escape from the struggle with passwords and the widely disliked two-factor authentication the banks inflict on them [7].

There is need to identify biometrics technologies and systems that provide superior security and privacy along with ease of use to integrate them in e-banking and e-business. Research on similar lines was carried out by Carnegie Melon's Biometrics Center, which has developed a technology that can identify a human from 40 feet away just by scanning the person's irises[8].

The current study concerns about evaluating the performance of different biometric technologies so as to find the most practically viable solutions with very equitable results for implementation in important areas of application and in the current study performance evaluation of different biometric technologies it is done based on the identified combined significant metrics for implementation biometrics in various e-banking channels.

II. REVIEW OF LITERATURE

The research has been going on for number of years to increase the performance of biometric systems, so as to make them practically viable and there have been very satisfactory results in a number of areas, which can be implemented in various e-banking channels.

The performance of any system is expressed by some parameters and similarly the performance of a biometric system can be expressed in FAR (False Acceptance Rate), FRR (False Rejection Rate), GAR (Genuine Accept Rate), and EER (Equal Error rate). A FAR of zero means that no imposter is accepted as genuine individual. GAR is used to measure the accuracy of a biometric system. A decision made by a biometric system is either a — genuine individual-type of decision or a — imposter type of decision.

Marco Gamass et al. in their study present a critical analysis of the measurement of accuracy and performance of a biometric system, they propose as well as discuss a methodology for the measurement of the accuracy of biometric systems with not-symmetric matching function [9].

Anil K. Jain et al in their study give a brief comparison of biometric technologies based on seven factors and rate them are per the perception of the authors [10].

Alina Klokova in her study performs the comparison analysis of widely used biometric identifiers and their recognition techniques with the comparison criteria list presented is limited to universality, distinctiveness, permanence, collectability, performance, acceptability, circumvention and cost [11].

Sanjay Kumar et al. in their study provides an overview of the different biometric technique with some advantages and disadvantages in order to try and find out which technique is more reliable and secure[12].

Almayyan, Waheeda in their thesis propose a novel fusion approach at a hybrid level between iris and online signature traits as multimodal system and investigate the relative performance of several statistical data fusion techniques for integrating the information in both unimodal and multimodal biometrics by comparing the results of the multimodal approach with the results of the individual online signature and iris authentication approaches [13].

C.B. Tatepamulwar and Dr. V. P. Pawar compare different physiological and behavioral biometrics based on different criteria's like Uniqueness, Universality, Permanence, Circumvention, Performance, Collectability and Distinctiveness[14].

Precise Biometrics in its white paper does Biometric performance evaluation by performing many genuine and impostor comparisons and analyzing produced similarity scores or match decisions[15].

Gursimarpreet Kaur and Dr. Chander Kant Verma compare various biometric modalities are based on different perspectives like Basic metrics (Uniqueness, Universality, Permanence, Circumvention, Performance, Collectability and Distinctiveness), Metrics based on social view (Socially introduced, Privacy concept, Hygiene factor, Safety, Cost, Popularity, Ease of use) Metrics Based on evaluation (False acceptance rate, False rejection rate, Crossover error rate, Failure to enroll rate, Failure to capture rate, receiver operating char, Sensor subject distance) and metrics based on technical point of view (Processing speed, Accuracy, Template size, Device used, Technology used in device, Stability) [16].

Raju, A. S., and V. Udayashankara in their study explain that though unimodal biometric systems provide a very good result but they fail in certain conditions such as noisy acquisition, missing out of unique human characteristics etc. therefore there is need for a more robust biometric system. The study describes major technological perspective and fundamental progress in unimodal and multimodal biometric system as well as reviews the modalities of biometric system, biometric classification methods, past experimental results, merits and demerits of unimodal system and describes the integration scenario of multimodal biometrics[17].

R. Divya and V. Vijayalakshmi in their study state that multibiometrics is advantageous over unibiometrics as it is resilience to spoofing and has low False Acceptance Rate (FAR) and discuss the concept of biometrics and biometric system, multimodal biometric fusion techniques, crypto-biometrics and an algorithm for session key generation for secure communication of data[18].

The research gap is that most studies compare the performance of different biometric systems based on basic metrics and some based on different perspectives but none of the studies have aimed at conducting performance analysis of different biometric technologies based on significant metrics for biometrics based on the analysis of the concerns, opinions and perceptions of bankers, customers and technologists for deployment of biometrics in e-banking.

III. OBJECTIVES OF THE STUDY

The study was carried out with the aim to conduct performance analysis for the different biometric technologies presently available based on the identified combined significant metrics for biometrics deployment in E-Banking.

IV. RESEARCH METHODOLOGY

The study is pursued by assimilating information through a literature review for identifying the various types of biometric technologies presently available as well as to identify the significant metrics affecting their performance based on the analysis of the concerns, opinions and perceptions of bankers, customers and technologists for deployment of biometrics in e-banking, conclusively a performance analysis is conducted on the identified biometric technologies based on the identified combined significant metrics.

Performance Analysis Tool: Analytical Tool: MATLAB R2007b

V. ANALYSIS, FINDINGS AND CONCLUSION

The various types of biometric technologies available as on-date is as below:

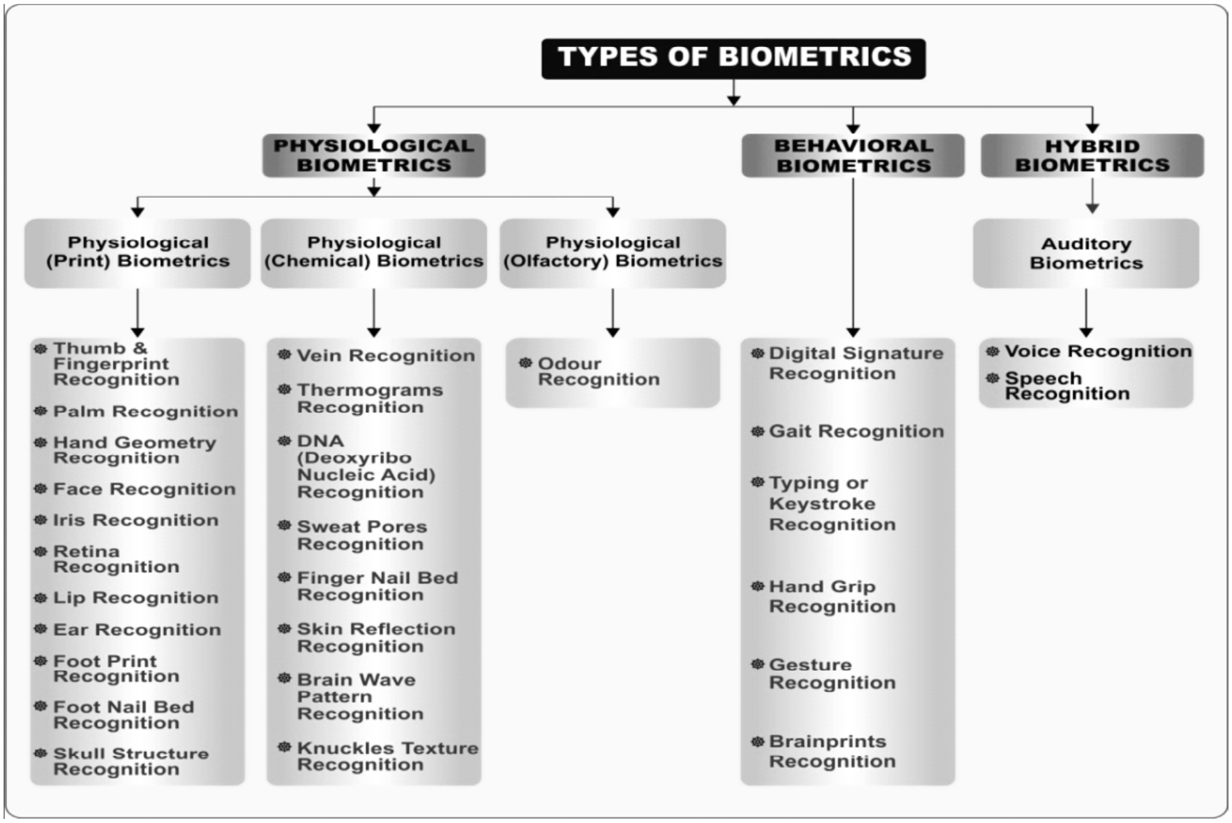
TYPES OF BIOMETRICS
PHYSIOLOGICAL BIOMETRICS
BEHAVIORAL BIOMETRICS
HYBRID BIOMETRICS
Physiological (Print) Biometrics
Physiological (Chemical) Biometrics
Physiological (Olfactory) Biometrics
Auditory Biometrics
Thumb & Fingerprint Recognition
Palm Recognition
Hand Geometry Recognition
Face Recognition
Iris Recognition
Retina Recognition
Lip Recognition
Ear Recognition
Foot Print Recognition
Foot Nail Bed Recognition
Skull Structure Recognition
Vein Recognition
Thermograms Recognition
DNA (Deoxyribo Nucleic Acid) Recognition
Sweat Pores Recognition
Finger Nail Bed Recognition
Skin Reflection Recognition
Brain Wave Pattern Recognition
Knuckles Texture Recognition
Odour Recognition
Digital Signature Recognition
Gait Recognition
Typing or Keystroke Recognition
Hand Grip Recognition
Gesture Recognition
Brainprints Recognition
Voice Recognition
Speech Recognition

Figure 1: The Various Types of Biometric Technologies Available as on Date [19]

Any human physiological or behavioral characteristics can become a measurable biometric characteristic provided it has the following basic properties: Universality, Uniqueness, Permanence, Acceptability and Collectability.

The significant metrics for deployment of Biometrics in E-banking from the assessment of concerns, opinions and perceptions of Banker’s are Technology Reliability, Performance, Circumvention Resistance, User Acceptability, Implementation Cost, Ergonomics and Training Requisite[20].

The significant metrics for deployment of Biometrics in E-banking from the assessment of concerns, opinions and perceptions of Customers are Reliability, Performance, Circumvention Resistance, Ergonomics, Minimum User Participation, Privacy Issues, Health Concerns, Data Security and Trust[21].

The significant metrics for deployment of Biometrics in E-banking from the assessment of concerns, opinions and perceptions of Biometric Technologists are Performance, Circumvention Resistance, Collectability, Size and Comparability, Minimum Operational Limitations, Intrusion Level and Portability[22].

The combined significant metrics for deployment of biometrics in e-banking are as illustrated in Figure 2:

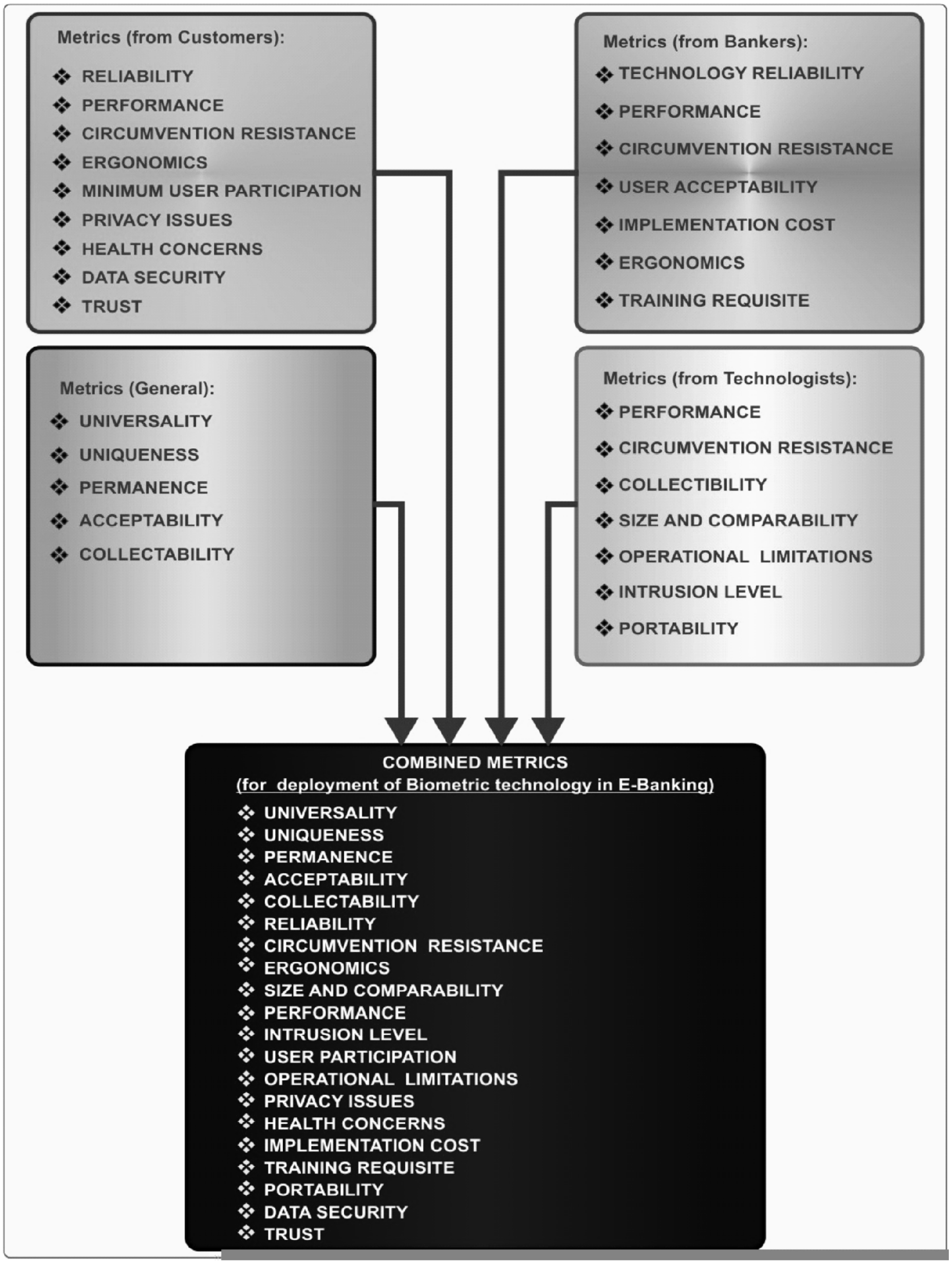

Figure 2: Combined Metrics for Deployment of Biometric Technology in E-banking [Self Adaptation]

The performance analysis for the various biometric technologies available as on-date is carry out by rating them for each metrics (only the two metrics Data Security and Trust are excluded, as these factors are technology independent and dependent on the organization implementing the technology), the summary of findings are as below:

VI. CONCLUSION

The results of performance analysis based on combined significant metrics for the various biometric technologies available as on-date shows that the biometric technologies that are currently the most suitable for deployment in e-banking are:

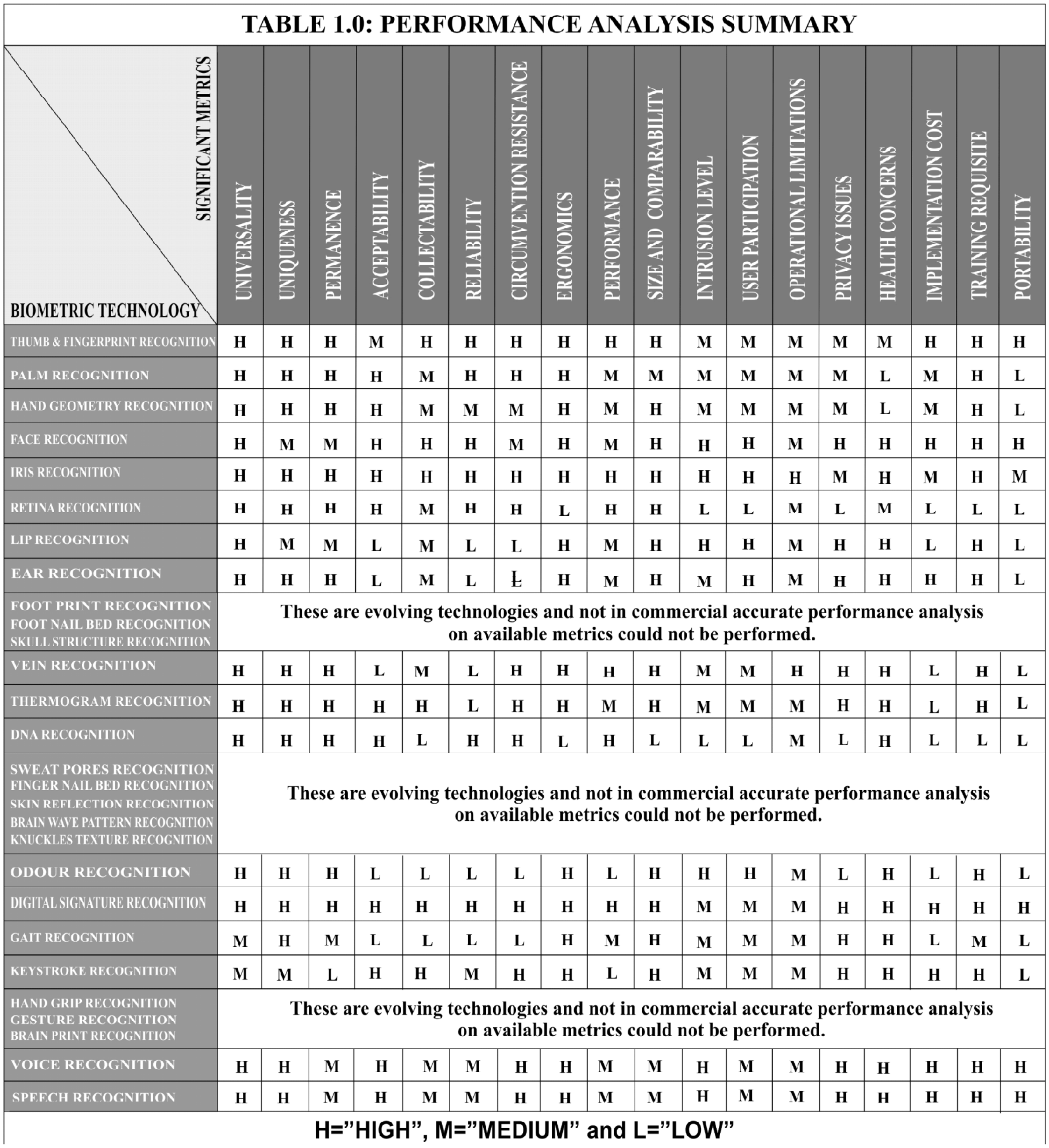

TABLE 1.0: PERFORMANCE ANALYSIS SUMMARY

SIGNIFICANT METRICS BIOMETRIC TECHNOLOGY	UNIVERSALITY	UNIQUENESS	PERMANENCE	ACCEPTABILITY	COLLECTABILITY	RELIABILITY	CIRCUMVENTION RESISTANCE	ERGONOMICS	PERFORMANCE	SIZE AND COMPARABILITY	INTRUSION LEVEL	USER PARTICIPATION	OPERATIONAL LIMITATIONS	PRIVACY ISSUES	HEALTH CONCERNS	IMPLEMENTATION COST	TRAINING REQUISITE	PORTABILITY
THUMB & FINGERPRINT RECOGNITION	H	H	H	M	H	H	H	H	H	H	M	M	M	M	M	H	H	H
PALM RECOGNITION	H	H	H	H	M	H	H	H	M	M	M	M	M	M	L	M	H	L
HAND GEOMETRY RECOGNITION	H	H	H	H	M	M	M	H	M	H	M	M	M	M	L	M	H	L
FACE RECOGNITION	H	M	M	H	H	H	M	H	M	H	H	H	M	H	H	H	H	H
IRIS RECOGNITION	H	H	H	H	H	H	H	H	H	H	H	H	H	M	H	M	H	M
RETINA RECOGNITION	H	H	H	H	M	H	H	L	H	H	L	L	M	L	M	L	L	L
LIP RECOGNITION	H	M	M	L	M	L	L	H	M	H	H	H	M	H	H	L	H	L
EAR RECOGNITION	H	H	H	L	M	L	L	H	M	H	M	H	M	H	H	H	H	L
FOOT PRINT RECOGNITION FOOT NAIL BED RECOGNITION SKULL STRUCTURE RECOGNITION	These are evolving technologies and not in commercial accurate performance analysis on available metrics could not be performed.																	
VEIN RECOGNITION	H	H	H	L	M	L	H	H	H	H	M	M	H	H	H	L	H	L
THERMOGRAM RECOGNITION	H	H	H	H	H	L	H	H	M	H	M	M	M	H	H	L	H	L
DNA RECOGNITION	H	H	H	H	L	H	H	L	H	L	L	L	M	L	H	L	L	L
SWEAT PORES RECOGNITION FINGER NAIL BED RECOGNITION SKIN REFLECTION RECOGNITION BRAIN WAVE PATTERN RECOGNITION KNUCKLES TEXTURE RECOGNITION	These are evolving technologies and not in commercial accurate performance analysis on available metrics could not be performed.																	
ODOUR RECOGNITION	H	H	H	L	L	L	L	H	L	H	H	H	M	L	H	L	H	L
DIGITAL SIGNATURE RECOGNITION	H	H	H	H	H	H	H	H	H	H	M	M	M	H	H	H	H	H
GAIT RECOGNITION	M	H	M	L	L	L	L	H	M	H	M	M	M	H	H	L	M	L
KEYSTROKE RECOGNITION	M	M	L	H	H	M	H	H	L	H	M	M	M	H	H	H	H	L
HAND GRIP RECOGNITION GESTURE RECOGNITION BRAIN PRINT RECOGNITION	These are evolving technologies and not in commercial accurate performance analysis on available metrics could not be performed.																	
VOICE RECOGNITION	H	H	M	H	M	M	H	H	M	M	H	M	M	H	H	H	H	H
SPEECH RECOGNITION	H	H	M	H	M	M	H	H	M	M	H	M	M	H	H	H	H	H

H=”HIGH”, M=”MEDIUM” and L=”LOW”

- Thumb & Fingerprint Recognition
- Speech Recognition
- Face Recognition
- Iris Recognition
- Digital Signature Recognition
- Voice Recognition

ACKNOWLEDGMENT

I acknowledge the assistance of Prof. Anoop Swarup (VC- Jagran Lake City University, Bhopal, INDIA) and Dr. Sohan Garg (Director- Sir Chotu Ram Institute of Engineering and Technology, C.C.S. University, Meerut, U.P. INDIA)

APPENDIX

File containing all the Tables and Figures used in the paper as an addendum.

REFERENCES

[1] Munish Sabharwal (Shobhit University, INDIA (Ph.D Thesis)), “An Analytical evaluation of the design and implementation of computerization by Banks in India”, 2013.

[2] Edmund Spinella (SANS GSEC Institute , San Francisco, CA), “Biometric Scanning Technologies: Finger, Facial and Retinal Scanning”, 28 May 2003.

[3] Wayman, J., D., M., & Maio., “Biometric Systems –Technology, Design and Performance Evaluation”, London: Springer-Verlag British Library (*ISBN*978-1-84628-064-1) 2005 pp. 58.

[4] Prof. Selina Oko (Department of Computer Science, Ebonyi State University Abakaliki, Nigeria and Jane Oruh, Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Nigeria), “Enhanced ATM Security System Using Biometrics”, International Journal of Computer Science Issues (ISSN (Online): 1694-0814), Vol. 9, Issue 5, No 3, September 2012 pp. 352-357.

[5] S.T. Bhosale & Dr. B.S.Sawant, “Security in E-Banking via card less Biometric ATMs”, International Journal of Advanced Technology & Engineering Research (ISSN No: 2250-3536), Volume 2, Issue 4, July 2012 pp. 9-12.

[6] Source: “First facial recognition ATM developed in China”, The Hindu, Published: 31st May 2015.

[7] Angela Sasse (Professor at Universty College London and director of the UK Research Institute in Science of Cyber Security), “The question: when will biometrics take over from passwords? “, Published: April 2015 <http://www.theguardian.com/technology/2015/apr/13/biometrics-take-over-passwords-security-iphone>

[8] Daniel Bean, “New Iris Scanning Tech Could Identify You from 40 Feet Away”, Yahoo Tech, Published: April 18, 2015, <https://www.yahoo.com/tech/new-iris-scanning-tech-could-identify-you-from-40-116671805404.html>

[9] Marco Gamassi, Massimo Lazzaroni, Mauro Misino, Vincenzo Piuri, Daniele Sana, Fabio Scotti, “Accuracy and Performance of Biometric Systems”, IMTC 2004 – Instrumentation and Measurement Technology Conference Como, Italy, 18-20 May 2004.

[10] Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, NO. 1, January 2004.

[11] Alina Klokova, “Comparison of various Biometric Methods”, Interactive Multimedia Systems, Electronics and Computer Science, University of Southampton, 2010.

[12] Sanjay Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1595-1597.

[13] Almayyan, Waheeda. “Performance analysis of multimodal biometric fusion.” Journal of Computer Science 2012 290-296.

[14] Ms. C.B. Tatepamulwar, Dr. V. P. Pawar, “Comparison of Biometric Trends Based on Different Criteria”, Asian Journal of Management Sciences, 02 (03 Special Issue); 2014, 159-165.

[15] Precise Biometrics, White Paper- Understanding Biometric Performance Evaluation, 2014.

[16] Gursimarpreet Kaur and Dr.Chander Kant Verma, “Comparative Analysis of Biometric Modalities”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 4,April 2014

[17] Raju, A. S., and V. Udayashankara. “Biometric person authentication: A review.” Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014. Institute of Electrical and Electronics Engineers Inc., 2014. 575-580. Print.

[18] Divya, R., and V. Vijayalakshmi. “Analysis of multimodal biometric fusion based authentication techniques for network security.” International Journal of Security and its Applications 9.4 (2015) : 239-246. Print.

[19] Munish Sabharwal et. al., “The summation of potential biometric types and technologies for authentication in e-banking”, International Journal for Scientific Review and Research in Engineering and Technology, ISSN (online): 2455-3603, Vol. 1, Issue 2, pp. 83-92, Feb 2016.

[20] Munish Sabharwal, “The assessment of concerns, opinions and perceptions of Banker’s to find the significant metrics for deployment of Biometrics in E-banking” CiiT International Journal of Biometrics and Bioinformatics, ISSN 0974 – 9659 (Print) ISSN 0974 – 955 (Online), Vol. 8, Issue 2, pp.1-11, Feb 2016.

[21] Munish Sabharwal, “The assessment of concerns, opinions and perceptions of Customers to find the significant metrics for deployment of Biometrics in E-banking”, International Journal of Computer Applications (IJCA), ISSN 0975-8887 Impact Factor -0.715, Vol. 138, Issue 14, pp. 28-41, April 2016.

[22] Munish Sabharwal, “The assessment of concerns, opinions and perceptions of Biometric Technologists to find the significant metrics for deployment of Biometrics in E-banking”, SM Journal of Biometrics & Biostatistics, accepted by SM Online Scientific Resources, USA for publication in June-July, 2016.