International Journal of Scientific Review and Research in Engineering and Technology (IJSRRET)
ISSN: 2455-3603
||Volume|| 1 ||Issue|| 1 ||Pages-05-10||

The Summation of Potential Biometric Types and Technologies for Authentication in E-Banking

[1,]Sabharwal, [2,]Sohan Garg
[1,]KITE Group of Institutions, Meerut (U.P.) INDIA.
[2,]Sir Chotu Ram College of Engineering & Technology C.C.S. Univ., Meerut, INDIA

ABSTRACT: The review paper is written with the objective to find the various different types of biometrics and the technologies within each type available as on-date that can be applied for authentication in e-banking. This study is pursued by performing a "KEYWORD SEARCH" on Journals, Articles, Published Thesis, Project Reports, Case studies related to biometrics as well as websites, brochures, products and services of biometric hardware and service providing companies, to collect information through a literature review. The study suggests the various different types of biometric types as well the technologies within each type available as on-date that can be used for authentication in e-banking.

KEYWORDS: Biometrics, Biometric Technology, Biometric Authentication, Physiological Biometric, Behavioral Biometric, Hybrid Biometric

I. INTRODUCTION

The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure). In his study he refers to biometrics as the technologies used to measure and analyze personal characteristics, both physiological and behavioural. 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.[1] Biometrics is an automated method of recognizing a person based on a physiological or behavioural characteristic. Biometric technologies are becoming an additional layer added to existing system. There are bundle of highly secure identification and personal verification solutions but it is much required to have a robust system, encountering the security breaches and transaction frauds.

Biometrics technologies are base for a plethora of highly secure identification and personal verification solutions. But there arises a need for more robust systems in order to tackle the increasing incidents of security breaches and frauds. So there is always a need for fool proof technology that can provide security and safety to individuals and the transactions that the individuals make. This study explores the need for biometrics in secure electronic banking, investing and other financial transactions.Security and privacy issues have remained a challenge for years. These become more crucial when it's about the security and privacy of data in electronic form. Personal identification (authentication) plays a vital role in modern society.[2] It can help in achieving the security by the identification of an individual.Information technology widely uses Passwords or Personal Identification Numbers (PIN's) to verify a user to a system. Recognition of a PIN does not, however, mean recognition of the person's identity. Anybody can have gained access to a PIN, a card or any other 'key' that is being used to get access to a device. 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. Biometrics could be used to gain trust to a device instead of PIN's or passwords. Also now with the wide use of IT and Gadgets one 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.

Authentication process can be performed, based on something you know (passwords and Pin's), something you have (ID card or Token) and something you are (biometrics). The two conventional methods of personal identification i.e. something you know and something you have (passwords and tokens), had limitations associated with them i.e. you do not remember what you knew and you do not have what you had.[3,4] The authentication mechanism, based on the biometrics technology, is used to prevent access to the critical information, installations and areas that are restricted.[5]

Today, biometric technologies are used in several verticals such as Banking, Government organizations, corporations, and so on, where security remains the prime concern. Biometrics is today introduced for identification by the Indian Government agencies in Aadhaar Card, Passports, and Driving Licenses etc. The banks are being forced to change rapidly as a result of forces such as threat of competition, customer demand, and technological innovations. E-banking becomes a necessity strategic tool for banks to remain competitive in the market, and provide integrated value added services for the customer. He says it is hard to imagine a bank without the e- banking technology. However, technological advancement are and will continue impact the banking environment, to make existing channels more efficient and support creating new channels like M-banking and T-banking.[6]

With the use of internet becoming indispensable not only in communication and business but specifically in e-banking and e-commerce, the user authentication is become mega important in today's technology dominant era and there is an imperative necessity for technologies have the potential to make authentication secure and foolproof. To cover the limitations associated with the conventional methods of authentication, a new authentication mechanism-based on what you are (biometrics) is introduced.

II. REVIEW OF LITERATURE

Biometrics technology involves measuring and storing of the physical and behavioural characteristics of an individual in order to identify that individual on the basis of the stored characteristics Biometrics characteristics are almost impossible to steal, cannot be forgotten and very difficult to forge.[2] A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic are Voice recognition, keystroke-scan, and signature- scan. In this paper different biometrics techniques such as Iris scan, retina scan and face recognition techniques are discussed.[7]

The recent advances in reliability and performance and cost drops make these technologies attractive solutions for many computer and network access, protection of digital content and physical access control problems. Biometric systems are used for verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic.[8] Biometrics technology provides the greater security and convenience in authentication process as compared to traditional identification methods.[9] Biometrics is a great way of authenticating users. The user may be authenticated by a workstation during the logon, by a smartcard to unlock the private key, by a voice verification system to confirm a bank transaction or by a physical access control system to open a door. All of these cases are typical and correct places where to deploy a biometric system.[10] Passwords are passe; fingerprints are falling out of fashion, enter body print, a new effort from Yahoo's Research Labs, which looks to transform users into walking, talking, Smartphone using passwords. Anything from ears to knuckles to the barest edge of fingertips can be used to unlock mobile devices.[11] Biometric technology makes sense for e-payment. In today's world, no one needs pockets. That stuff jingling around in there keys, credit cards, checkbooks are replaced by something closer to the body. When you need to open a door or make a purchase, technology allows anyone to do so with a fingerprint, a voice command, or a computer scan of eyeball. A new approach to the fingerprint payment technology i. e. using

biometric technology with E- payment is perfect because it won't just identify, but it will authenticate as well. Dilip Kumar and Yeonseung Ryu have suggested using fingerprint for operating ATMs, here in state of using the card, fingerprint get used for transaction. [12] The security and authentication for online application system by using OTP and Biometrics System of Fingerprint Scanning in daily life, use of banking applications is increased gradually. The security of such type of online applications is more important. Current online applications provide the security like security card, passwords for authenticating the user but do not provide more security for the users and are also not available for any emergency situations. In order to overcome the disadvantages of security cards, we will use OTP and Biometrics for Authentication of online application system.[13] Carnegie Melon's Biometrics Center has developed technology that can identify a human from 40 feet away just by scanning the person's irises.[14]

Chinese researchers have successfully developed the first automated teller machine (ATM) with facial recognition technology to reduce the risk of theft, media reports said. The developers include Tsinghua University and Tzekwan Technology, a Hangzhou firm in eastern China's Zhejiang province that provides security protection for financial transactions; South China Morning Post quoted Chinese official media as saying.[15] Over the years, biometric technology explored by several banks majorly aims at providing business solutions and best customer services. Bank of Central Asia, Indonesia incorporates fingerprint systems to secure the processing of high-value electronic fund transactions.[16] Chase Manhattan Bank utilizes voice recognition for bank transactions where customers enroll with a standard phrase and when entering the bank they go to a podium housing a modified telephone, swipe the bank card (identification), speak the standard phrase (verification) and then receive a receipt to present to the teller. One advantage of this is that the cashier is able to pull the customer's file before they get to the teller, hence conserving time.

Rawlson O`Neil King, Biometrics Research Group Inc in his white paper examines how the total market for mobile biometrics will increase due to Smartphone growth along with the drive for password supplantation. This report also outlines the increasing use of mobile biometrics for financial services and to aid in law enforcement and military applications.[17] Cross Match in their White Paper state that by adding biometrics, Banco Azteca experienced strong and sustained growth and quickly became one of the largest banks in Mexico with $6.1B in assets. Banco Azteca has also expanded its operations by offering highly profitable microfinance services in Honduras, Argentina, Panama, Peru and Brazil.[18]

Apple's Touch ID has certainly changed the perceptions of the decision makers in banking security, allowing biometrics to be a serious contender in providing authentication for banking services. There is also a role that biometrics could play in reducing the amount of fraud that is occurring for Apple Pay.[19] SK Telecom, South Korea has introduced voice biometrics in its call center for easy and secure authentication. The technology will streamline the authentication process by allowing customers to speak a simple passphrase to access their accounts, creating an easier and more personalized experience.[20] In the last two decades banks in India have embraced information and communication technology in a big way. They have migrated to core banking platform thereby seamlessly networking their bank branches across the country. This has helped banks to provide enhanced services and new products to their customers in a more efficient manner. The purpose of this research is to examine the alternate delivery channels available to bank customers for various banking services at their door step.[21]

One of the greatest challenges for banking and payments companies is verifying (or authenticating) their customers' identity. Banking and payments have long relied on personal identification numbers (PINs), usernames and passwords for this task. These are collectively termed authentication methods and are critical for online banking and POS interactions. As mobile and online services increase in popularity, customers are burdened with a growing list of passwords, usernames and PIN numbers to track everything from their brokerage to their Etsy account. Not only is the tracking of one's existing PINs, passwords and usernames becoming impossible to manage, but the process of creating and managing new authentication is as joyless as a sharp stick in the eye.[22]

III. OBJECTIVES OF THE STUDY

The review paper is written with the objective to find the various different biometric types and the technologies within each type available as on-date that can be applied for authentication in e-banking.

IV. RESEARCH METHODOLOGY

The study is pursued is pursued by performing a "KEYWORD SEARCH" on Journals, Articles, Published Thesis, Project Reports, Case studies related to biometrics as well as websites, brochures, products and services of biometric hardware and service providing companies, to collect information through a literature review.

V. DISCUSSIONS AND FINDINGS

Biometrics technology involves measuring and storing of the physical and behavioural characteristics of an individual in order to identify that individual on the basis of the stored characteristics Biometrics characteristics are almost impossible to steal, cannot be forgotten and very difficult to forge[2] The common physical biometrics techniques or "static biometrics" are fingerprint, face, retina, hand geometry, iris, palm, vein and DNA are hard to spoof, but they are static data that could be stolen and they also force users to go through another pesky step in the authentication process while the behavioral biometrics -- or "passive biometrics," like signature, gait, voice biometrics, mouse usage dynamics, navigation habits, keystroke dynamics like the speed with which you type and the pressure you hit the keys with, gesture dynamics like swipe speed and distance -- all things you do unconsciously which happen to be very unique to you. Physiological biometric are active biometrics produce static data about the identify of an individual therefore once stolen, they are stolen for lifetime and there is possibly in no way get back to a secure situation and worse yet, they force users to go through another pesky step in the authentication process.

Physiological biometric is further classified into three categories:

- Physiological (Print) Biometric includes 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 etc.
- Physiological (Chemical) Biometric includes Vein Recognition, Thermo grams Recognition, DNA (Deoxyribo Nucleic Acid) Recognition, Sweat Pores Recognition, Finger Nail Bed Recognition, Skin Reflection Recognition, Brain Wave Pattern Recognition, Knuckles Texture Recognition etc.
- Physical (Olfactory) Biometric includes Odour Recognition.

Behavioural biometric are passive biometrics produce dynamic data involving all things you do unconsciously which happen to be very unique to you. These imply "what can we observe, rather than request from people". These new technologies may monitor mouse dynamics, navigation habits, and keystroke dynamics, like the speed you type and the pressure you hit the keys with, gesture dynamics like swipe speed and distance -- all things you do unconsciously which happen to be very unique to you.

Behavioral biometric includes Digital Signature Recognition, Gait Recognition, Typing or Keystroke Recognition, Hand Grip Recognition, Gesture Recognition, Brain prints Recognition etc Hybrid biometrics are biometric that are a blend of physiological biometrics and Behavioural biometrics like voice recognition and speech recognition.

There are also some biometrics techniques that are in research pipe line e.g. ear biometrics, Lips shape biometrics, body prints, Brain prints etcAuditory Biometric includes Voice Recognition, Speech Recognition etc

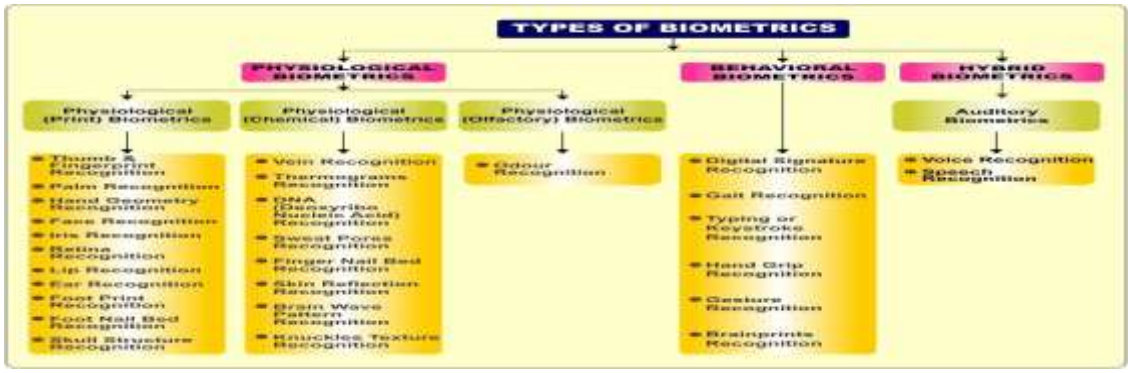

Figure 1: The Various Types of Biometric Technologies Available as on Date

ACKNOWLEDGEMENT

We acknowledge the guidance and review assistance of Prof. Anoop Swarup (VC- Jagran Lake City University, Bhopal, INDIA)

REFERENCES

1. Edmund Spinella (SANS GSEC Institute , San Francisco, CA), "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", 28 May 2003
2. Stanley, P., Jeberson, W., & Klinsega, V.V, "International Conference on Biometric Authentication: A Trustworthy Technology for Improved Authentication, in Future Network", 2009, pp. 171 – 175
3. Russell Kay, "QuickStudy: Biometric Authentication", 2009 Accessed: Nov 11, 2014], Available at:
4. <http://www.computerworld.com/s/article/100772/Biometric_Authentication>
5. Boatwright, M, & Luo, X., "What do we know about biometrics authentication?, In Proceedings of the 4th Annual Conference on information Security Curriculum Development", InfoSecCD '07, 2007 ACM, New York, pp. 1-5.
6. Flores Zuniga, Alejandro Enrique, Khin Than Win, and Willy Susilo, "Biometrics for electronic health records." Journal of Medical Systems (ISSN: 0148-5598 (Print) 1573- 689X (Online)), 2010 pp. 975-983
7. Adnan M. Al-Khatib (CIS Dept., College of IT, Jerash University, Jerash , Jordan), "E- Banking : Survey" International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X), Volume 2, Issue 10,October 2012 pp. 12 -19
8. Renu Bhatia(Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India) , "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X), Volume 3, Issue 5, May 2013 pp. 93-100
9. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K. and Senior, A. W., "Guide to Biometrics", New York: Springer, (ISBN: 8184891601, 9788184891607) 2003 pp. 3-5
10. Wayman, J.L., "Biometrics in Identity Management Systems", IEEE Security and Privacy (ISSN: 1540-7993) Vol.6, No.2, 2008 pp. 30-37
11. Vaclav Matyas and Zdenek Rıha (Faculty of Informatics, Masaryk University Brno,
12. Czech Republic), "Technical Report Biometric Authentication —Security and Usability"
13. , IEEE Security & Privacy (ISSN: 1540-7993), 2003
14. Douglas Bonderud, "Bodyprint Biometrics: Are People the New Password?", Published: April 28, 2015, available at : <http://securityintelligence.com/news/bodyprint-biometrics- are-people-the-new-password/?CT=ISM0056#.VZotBUYreM8>
15. Dilip Kumar & Yeonseung Ryu, "A Brief Introduction of Biometrics and fingerprint Payment Technology", Published by the IEEE Computer Society, 2008.
16. Namita Chandra, Ashwini Taksal, Dhanshri Shinde, Prof. Archana Lomte (Department of Computer, BSIOTR (W), Pune University, Maharashtra, India), "Sensitive Data Protection Using Bio-Metrics", International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X), Volume 4, Issue 1, January 2014,
17. pp. 1019-1025
18. 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>
19. Source: "First facial recognition ATM developed in China", The Hindu, Published: 31st May 2015
20. Krawczyk, S. and Michaud, C., "Biometrics in the Banking Industry", CSE 891.2005
21. Source: Rawlson O`Neil King, Lead Researcher, Biometrics Research Group, Inc., "White Paper: Mobile Biometric Authentication White Paper", Biometrics Research Group, Inc., 2013
22. Source: White Paper by CrossMatch: "Biometrics in banking from unbanked to lifelong customer" Published: January 2014
23. lan Goode, founder and managing director of Goode Intelligence, "Blog: Biometrics for banking gets going", Published: 02 June 2015, <http://www.planetbiometrics.com/article- details/i/2953/desc/blog-biometrics-for-banking-gets-going/>
24. Oksana Walton, "Telecom giant in South Korea uses voice biometrics to revamp the customer experience", Posted: April 28, 2015, <http://whatsnext.nuance.com/customer- experience/sk-telecom-announces-voice-biometrics-in-call-center/>

25. Dr. Mahalaxmi Krishnan (Associate professor of commerce, K J Somiya College of Arts & Commerce, Mumbai), "Alternate Banking Channels for Customer Convenience", International Journal of Scientific Research (ISSN No. 22778179), Volume 2, Issue 2, Feb 2013 pp. 9-10
26. Carron Oswald, "Biometrics – does your bank know you are you?", www.banknxt.com, Published: 6th April 2015, available at: <http://banknxt.com/49661/biometrics/>