SMGroup

SM Journal of Biometrics & Biostatistics

Research Article

The Assessment of Concerns, Opinions and Perceptions of Biometric Technologists to Find the Significant Metrics for Deployment of Biometrics in E-Banking

Dr. Munish Sabharwal[1]*

[1]*Executive Director and Professor, KITE Group of Institutions, Meerut (U.P.), India*

Article Information

Received date: Mar 11, 2016
Accepted date: Jun 07, 2016
Published date: Jun 15, 2016

***Corresponding author**

Dr. Munish Sabharwal, Executive Director and Professor, KITE Group of Institutions, Meerut (U.P.), India, Tel: +91-9927500592; Email: mscheckmail@yahoo.com

Keywords E-Banking; Biometric Technologies; Biometrics Deployment; Technologist Perception; Significant Metrics for Biometrics Implementation

Abstract

The research work was conducted with the objective to find the significant metrics for biometrics deployment in e-banking through an assessment of the concerns, opinions and perceptions of biometric technologists regarding the implementation of biometrics in e-banking.

This paper is pursued by collecting information through survey of technologists working with biometrics; the technologists are chosen using snowball sampling. Then the results of the surveys are analyzed to find the significant metrics for the deployment of biometrics technology in e-banking.

The study suggests that the overall significant metrics for the deployment of Biometric technology in E-Banking with the biometric technologists perspective are Performance, Circumvention Resistance, Collectability, Size and Comparability, Minimum Operational Limitations, Intrusion Level and Portability.

Introduction

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.

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.

The authentication mechanism, based on the biometrics technology, is used to prevent access to the critical information, installations and areas that are restricted [1].

The dependency of businesses in the form of e-commerce has increased manifolds, so has the use of internet, proportionately the frauds have also increased manifolds specifically in e-banking and e-business channels.

Brett Relander, [2] assert that with reports of data breaches becoming increasingly common, the lack of effective financial data security mechanisms has become a matter of serious concern. Among the most publicized of those breaches that have contributed to this growing concern are those which recently affected Home Depot (HD) and Target, but these are by no means isolated cases. Data breaches have become more and more frequent. According to the Identity Theft Resource Centre, to date there have been more than 778 million records exposed in thousands of data breaches.

HCL Technologies India [3] in its white paper on biometrics state that e-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. Banks are bound to use this combination to better authenticate customers and ensure non-repudiation of online banking, trading and purchasing transactions. Biometrics can help to obtain secure services over the telephone through voice authentication.

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.

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 centered on information and information processing, which themselves are highly Technology dependent [4].

Biometrics provides a high degree of security and convenience which ensures confidentiality of personal information [5].

This is superior to traditional passwords/PINs as these are easily guessed, forgotten, or copied; tokens can be stolen or misplaced [6]. Biometric technology helps in preventing theft as the information is stored in the form of a digital record in the database which makes it highly impossible to reconstruct, decrypt, or manipulate [7].

Biometric uses biological characteristics or features which are inseparable from a person, thus, reducing the threat of loss or theft [8].

Biometrics technology has remained controversial for invading the privacy of individuals. People, sometimes, have doubts and concerns about their privacy.

The critics of biometrics claimed biometrics as a threat to the individual's privacy [9].

Though biometrics has been implemented in many organizations but still there is a long way to go. It is very important that the responses, both perceived and behavioral, of the citizens and end users are considered when deigning and deploying system having digital identities [10].

Chandra and Calderon [11] explain the user's issues involved in the deployment of biometrics technology. They elaborate that if the people concerns i.e. trust, user acceptance, privacy concerns are not addressed then there is a potential threat to system failure. It would be surprising to deploy biometrics technology without measuring the people's perceptions about biometrics technology.

Using biometrics raises concerns about the public's perception of a possible intrusion of their privacy [12]. One can generally say that the less intrusive the biometric, the more likely it is that it will be accepted by the users.

Since the use of biometric technologies involves sharing of an individual's indispensable identity data, the opinions of users and bankers before their deployment must essentially be considered.

Review of Literature

Since the use of biometric technologies involves sharing of an individual's indispensable identity data, the opinions of users and bankers before their deployment must essentially be considered. According to Woodward [13] there are two different blogs of opinions about biometrics as it's a relatively new technology. The critics claims it as a privacy invader while the pro biometrics blog details and supports the biometrics technology for improved security and the greater services. People have concerns regarding their security and privacy when dealing with biometrics. In this paper the question (Is biometrics a privacy friend or privacy foe?) is answered by first explaining the biometrics technology and its expected uses in daily life. The privacy aspects of biometrics are analyzed from invader as well as protective perspective of biometrics. Though people have concerns regarding the biometrics but when analyzed, the biometrics was found to be a technology that improves the privacy as well as the security of the users.

Wayne Penny in SANS Institute in [14] suggests that two of the issues to be overcome with biometric systems and public acceptance are communications, by the vendors or implementers, and public perception of the technology. The individual must be able to understand the behavior of the system to assess its capabilities to protect information and function in an open and secure manner.

Salil Prabhakar *et al.* [15] in their study suggest that the use of biometrics indeed raises several privacy concerns. A sound trade-off between security and privacy might be necessary; but we can only enforce collective accountability and acceptability standards through common legislation. On the positive side of the privacy issue, biometrics provides tools to enforce accountable logs of system transactions and to protect individual's right to privacy.

Chandra and Calderon [11] discussed the challenges and difficulties that biometrics technology face in becoming the core technology for authentication in information systems. Different types of challenges and issues i.e. business issues, operational issues and the people issues are studied. There is a need to approach these challenges in a way that satisfies the user concerns.

Elliot *et al.* [16] used the survey methodology in order to understand and analyze the citizen's perceptions, opinions and concerns of biometrics technology. The issues like security, safety and privacy concerns were asked in the survey. The results mentions that the people were pro biometrics i.e. they agreed that biometrics usage will enhance security but most of the respondents had concerns about the their privacy (who will use that data and how it is made sure that only the authentic people use that data). People seemed welcoming to biometrics technology but also they had safety concerns from using biometrics technology i.e. iris and scan technology. In short the people were willing to use biometrics technology but there was a certain lack of trust with some governmental institutes. There is also a need to educate people about the biometrics as most of the concerns can be removed if proper guidance and education is delivered about biometrics technology.

The research work of Furnell and Evangelatos [17] also explains the people perceptions about biometrics technology. The survey conducted by the researchers revealed that there is a certain level of acceptance towards biometrics among people. Moreover the survey states that TV, Newspapers and Internet are the sources that people get information of biometrics technology from. People were found having concerns of health risks while using biometrics devices. Privacy concerns, like who will access our stored data and how it will be used, were noticeable among people. They survey summarize that

although there is an adequate user acceptance for biometrics with certain concerns, there is a need to take steps for the awareness of people about their perceived concerns.

A. Pooe [18] in his study aimed to identify factors impacting on the adoption of biometric authentication in the South African banking sector as a means of authentication. The study constitutes exploratory research and is limited to the use of biometric technology within the financial services sector. Within this sector, specific focus is placed on the four leading South African banks. A survey was conducted, and the findings show common agreement and acceptance of biometric authentication as a way to improve information security in the various banking channels despite its not being widely implemented. With regard to factors influencing the adoption of biometric authentication, the study identified three main adoption inhibitors. This study contributes to the greater body of knowledge on the use of biometrics for banking applications by providing insight into current practices and perceptions.

Seyyede Samine Hosseini and Dr. Shahriar Mohammadi [19] in their study investigated the employees' and customers' conceptualizations about the introduction and accomplishment of a biometric authentication system in Saman bank of Shiraz, Iran and concluded that although the participants are aware of biometric technology's benefits, they believe that cultural and economic problems could be the two obstacles for implementation of such an authentication system in the banks of Iran.

Sookeun Byun and Sang-Eun Byun [20] in their study investigate multiple aspects of the benefits and risks that consumers perceive in using biometric technology. A survey was conducted by contacting the actual customers of an American bank that has utilized fingerprint technology at its ATMs. Banks thus may highlight intrinsic values, such as the novelty of biometrics, to motivate the use of the technology. However, to promote potential users' adoption decisions, banks need to educate them about the security benefits of financial transactions under the technology. The result also showed that the current users were highly concerned about information privacy risk in using the fingerprint ATMs. Therefore, banks are advised to develop internal policies to protect personal biometric data from any identity theft or illegal uses to encourage continuous usage by the current users.

Adewale Adeyinka A *et al.* [21] in their empirical evaluation capture the factors influencing the perception of the bank management and users. The analysis of the survey of 740 respondents cutting across different age groups and educational backgrounds showed that management and customers of strongly support the adoption of biometric ATM in Nigeria.

There have been several studies that have assessed the concerns, opinions and perceptions of bank employees as well as bank customers regarding use of biometrics in banking, the research gap is that none of the studies have specifically aimed at finding significant metrics for deployment of biometric in e-banking by assessing the concerns, opinions and perceptions of biometric technologists.

Objectives of the Study

The research work was conducted with the following objectives:

- To assess the concerns, opinions and perceptions of Biometric Technologists regarding the implementation of biometrics in e-banking
- To find the significant metrics for biometrics deployment in e-banking as per biometric technologists perspective

Hypothesis

Null Hypothesis or Ho = There is no significant difference in the responses of Male and Female Biometric Technologists.

Alternate Hypothesis or HA = There is significant difference in the responses of Male and Female Biometric Technologists.

Research Methodology

Survey method is used to identify and analyze the concerns, opinions and perceptions of technologists regarding the deployment of biometric technology in e-banking.

The technologists are chosen using snowball sampling.

Sample size for Technologists- 100

Data Collection

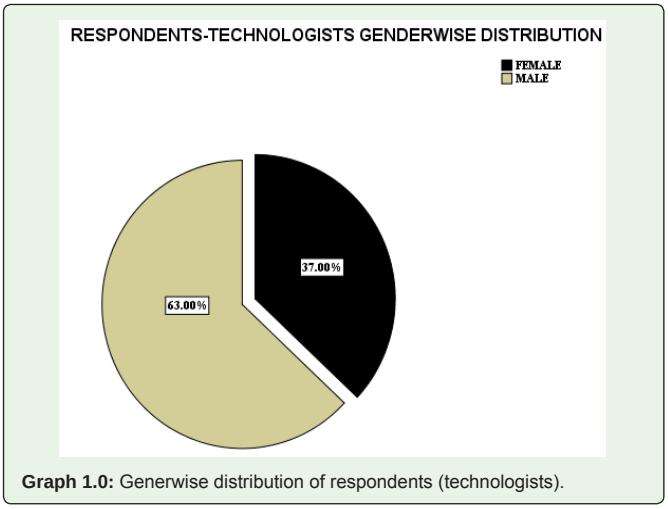
The researcher surveys the technologists working with biometrics to collect primary data. The respondents are asked to complete the questionnaire by verbally responding to questions in the presence of the researcher.

Discussions and Findings

The assessment of the concerns, opinions and perceptions of biometric technologists, regarding implementation of biometrics in e-banking by analyzing the survey data of technologists (100), collected using open ended questionnaire, the collected data is then assembled using Thematic Textual Analysis and finally Factor Analysis was run on the sample to find the significant metrics for deployment of biometrics in e-banking with technologists perspective.

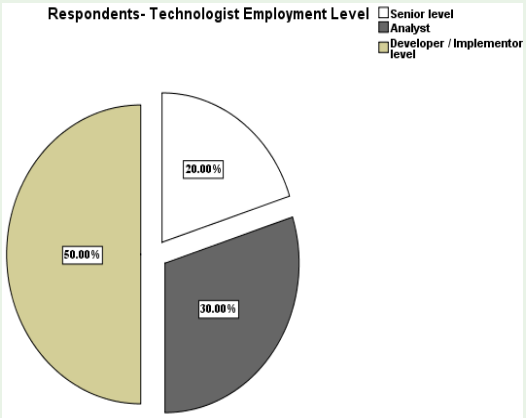
Introductory Questions

The graph 1.0 given below shows Gender wise distribution of respondents (Technologists), 63% of respondents are Male and 37% respondents are Female:



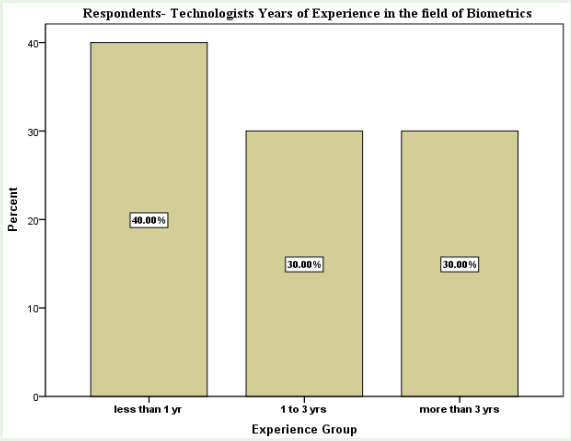
Graph 1.0: Generwise distribution of respondents (technologists).

The graph 2.0 given below shows employment level wise distribution of respondents (Technologists):



Graph 2.0: Employment level wise distribution of respondents (technologists).

The graph 3.0 given below shows the experience level distribution of respondents (Technologists):



Graph 3.0: Experience level wise distribution of respondents (technologists).

The Graphs 1.0, 2.0 and 3.0 clearly imply that the selected sample represents a holistic picture of the respondents.

Domain Specific Question

The researcher performs thematic textual analysis of the responses to the questionnaire by technologists; this yields the table (Table 1).

Finding Significant Metrics (as per technologist's perspective)

One-way ANOVA was applied on the dataset as per Table 1; the SPSS output is as below:

ANOVA					
FREQUENCY					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	868.056	1	868.056	4.323	.054
Within Groups	3212.889	16	200.806		
Total	4080.944	17			

Table 1.0: Summary of Thematic Textual Analysis of responses by technologists for the deployment of biometric technology in e-banking.

S. No.	Metrics	Frequency (n)	
		Male	Female
1	Performance	57	33
2	Circumvention Resistance	53	31
3	Collectability	42	28
4	Intrusion Level	41	24
5	Size and Comparability	37	22
6	Portability	31	18
7	Minimum Operational Limitations	27	16
8	Implementation Cost	12	5
9	Health Concerns	6	4

As Significance value or P > 0.05, H0 is accepted and HA is rejected; hence there is no significant difference in the responses of Male and Female Biometric Technologists.

Finally, Factor analysis was run on the sample to find the significant metrics for deployment of biometrics in e-banking as per the perceptions of biometric technologists and the extraction method used was Principal Component Analysis (PCA) with Varimax Rotation Method.

The seven significant metrics for deployment of biometrics in e-banking by assessing the concerns, opinions and perceptions of biometric technologists as supported by the results of factor analysis are Performance, Circumvention Resistance, Collectability Intrusion Level, Size and Comparability, Portability, Minimum Operational Limitations whereas Implementation Cost, Health Concerns were not found to be a significant metrics in the deployment of biometrics in e-banking as per biometric technologists.

The significant metrics for the deployment of Biometric technology in E-Banking with the technologist perspective are:

- Performance
- Circumvention Resistance
- Collectability
- Size and Comparability
- Minimum Operational Limitations
- Intrusion Level
- Portability

Acknowledgement

Author thanks and acknowledges the review 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

The copy of the Sample Survey Questionnaire for Biometric Technologists and a file containing all the Graphs, figures and tables used the paper as an addendum.

References

1. Flores Zuniga AE, Win KT, Susilo W. Biometrics for electronic health records. J Med Syst. 2010; 34: 975-983.
2. Relander B. Biometric Banking: Huge Prospects for Tech Profits. Investopedia. 2015.
3. HCL Technologies, India. White Paper: Biometrics-A Vision for the Future. 2011.
4. Sabharwal M. An Analytical evaluation of the design and implementation of computerization in Banking sector in India. Shobhit University. 2013.
5. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Trans Circuits Syst. Video Technol. 2004; 14: 4-20.
6. Jain AK, Ross A, Pankanti S. Biometrics: A Tool for Information Security. IEEE Trans Inf Forensics Secur. 2006; 1: 125-143.
7. Toth B. Biometric Liveness Detection. Information Security Bulletin, Chi Publishing. 2005; 10: 291-298.
8. Andy A, Schuckers S. Biometric Vulnerabilities, Overview. In: Encyclopedia of Biometrics. Springer. 2009; 160-168.
9. Arigbabu OA, Ahmad SMS, Adnan WAW, Yussof S. Recent advances in facial soft biometrics. Vis Comput. 2015; 31: 513-525.
10. Dwivedi A, Bali RK, Belsis MA, Naguib RNG, Every P, et al. Towards a practical healthcare information security model for healthcare institutions. Information Technology Applications in Biomedicine. 2003; 114-117.
11. Chandra A, Calderon, T. Challenges and constraints to the diffusion of biometrics in information systems. Communications of ACM. 2005; 48: 101-106.
12. Malallah FL, Ahmad SMS, Adnan WAW, Yussof S, Iranmanesh V, Arigbabu OA. A Review of Biometric Template Protection Techniques for Online Handwritten Signature Application. Int Rev Comput Softw. 2013; 8: 1-9.
13. Woodward JD. Biometrics: Privacy's foe or Privacy's friend? Proceedings of the IEEE. 1997; 85: 1480-1492.
14. Penny W. Biometrics: A Double Edged Sword -Security and Privacy. SANS Institute. 2002.
15. Prabhakar S, Pankanti S, Jain AK. Biometric Recognition: Security and Privacy Concerns. The Ieee Computer Society. 2003; 1: 33-42.
16. Elliott SJ, Massie SA, Sutton MJ. The Perception of Biometric Technology: A Survey. Automatic Identification Advanced Technologies. IEEE Workshop. 2007; 259-264.
17. Furnell S, Evangelatos K. Public awareness and perceptions of biometrics. Computer Fraud & Security. 2007; 2007: 8-13.
18. Pooe A, Labuschagne L. Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation. Southern African Business Review. 2011; 15: 119.
19. Hosseini SS, Mohammadi S. Acceptance of Banking on Biometric in Iran's Banking System Case Study of Saman Bank. J Basic Appl Sci Res. 2012; 2: 12744-12751.
20. Byun S, Byun SE. Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters. Behaviour & Information Technology. 2013; 32: 217-230.
21. Adeyinka AA, Ayodotun SI, Joke B, Tiwalade O, Anthony UA. Biometric Enabled E-Banking in Nigeria: Management and Customers' Perspectives. Information and Knowledge Management. 2014; 4: 23-38.