



Awareness of the employees of the banks regarding the implementation of biometric system in the banks

Jaskiranjit Kaur

Research Scholar, Department of Computer Engineering
Punjabi University, Patiala
India
er.jaskiran@gmail.com

Gaurav Gupta

Department of Computer Engineering
Punjabi University, Patiala
India
gaurav_shakti@yahoo.com

Abstract - The IT sector has played a major role in this century and has even proved as a beneficiary also. But everything has its own plus and minus points. So much of advancement in the IT sector has increased the sense of insecurity among all. This has led banks to increase security related to all types of transactions and ensuring that only the authenticated users are only using it because this only can determine the level of trust of a customer for a particular bank. This all requires a very strong and safe method that provides the best security to the customers. Biometric authentication method is one such way of increasing security and is being used globally. But this can be only done with the mutual consent of the employees of the bank which solely depends upon their compatibility with the new system. The following portion deals with the introduction and implementation of biometric system and the adaptability of the people dealing with it. Further its adaptation by the public sector and private sector banks.

I. INTRODUCTION

First and foremost thing for an organization for its uprising and building its image over people is by winning their trust. It is important for every organization to work primarily on the customer relationships for its healthy progress. For financial institutions it's a great challenge to build faith because of their major role to the economic development. The banks need to ensure that customer's money is at a safe place. It is not so difficult to win over the customer's reliability over the bank provided the bank has better security services to offer. But since there are some other factors as well which force the bank to give its customers utmost importance and thereby ensuring no chances of loopholes. With the advancements in the IT field, the security of the customers' should be the primary focus of the bank.

Bio metric system

This system verifies one's identity by taking under consideration one or more physical traits and then access is provided only this basis to the user. This system of verification seems to be safe because every individual has its own unique personal traits. So, no other can change the traits of other and hence there are no chances of security threat. (Jain et al, 2011). Some of them include scanning one's heart beat, iris can or fingerprints.

It is widely used in forensic applications, financial sector, passport service and even in healthcare sector (Drygajlo, 2006). Thus it is rightly said that biometric method is one of the most secure and safe technique of ensuring the customer safety.

Usage of bio metric system

It is the duty of the bank to protect the information from all unwanted intruders. Legislators have been encouraging banks to increase the status of their protection schemes due to increasing number of thefts but still many banks are continuing to use the obsolete system for their protection which makes it easy for the hackers to attack the bank. (Litan 2004). IT is but obvious that the unique identification of an individual can help in eliminating many cases of the fits (Jain et al, 2011). Therefore a bank must always keep changing and updating its system as per the changing scenario.

Advantages of bio metric system

The traditional methods of security as the token system and use of passwords are no longer sufficient enough to ensure safety. According to (O'Gorman, 2003), there can be many types of attacks possibly. Some of them are (Trojan Horse, Replay Attack, Host Attack, Phishing Attack, Brute Force Attack, Eavesdropping, Host Attack, Denial of Service etc) which can be easily caused due to methods such as password protection etc. further it is a beat method since it is user-friendly, convenient method of security and they also don't burden the users to remember passwords or transaction id's etc.

II. LITERATURE REVIEW

Internet has almost reached in every hands now but it has also made so difficult to ensure security for the information over the net. For the promotion of internet banking among the customers it is necessary to ensure first that security is not being compromised with. The study which was conducted by Lee (2006), a new research was found that showed the level of acceptance by the banks to accept the online banking system. Further it was found that the people who used this widely are youth who use it for greater amount of transaction allowed by the banks (like online shopping of various products e.g. clothes, food etc).

According to Byun (2013), e-banking concept only gets fulfilled only when the quality of the schemes offered is matching with the needs of the customers. Further Margulis,



(2011) also stated the ease with which bank system is being used, assuring safe transactions keeping in pace with the speed of the network. All these features has popularized the online banking system among all.

The preference of customers for choosing online banking over others is the dependent upon the customer relationship management. Rhea, (2002), the primary aim of bank is to provide a sound environment which provides safety in terms of money transactions. The contributing factors of building trust over customers are accountability, integrity and maintaining confidence. Therefore banks have a very fine security policy by focusing the above factors and also using various physical instruments like access cards and automated monitoring system that makes sure the right kind of information being entered and moved out.

Madu and Madu (2002) Stated that private information of the customers should be secured properly because this can be a major reason of their dissatisfaction. People are not aware much about the functioning of the system thus it becomes difficult to convince them for its security.

Ihejihi (2009) was concerned about the cases of ATM scams and inability of the bank to be answerable to the customers. According to him, banks must have very high level of security and should protect its customers against all kinds of thefts.

Obiano (2009) was concerned about the distribution of ATM cards among the customers which is being done without proper knowledge of the ways the card can be utilized. This leads to careless nature of customers towards the important details related to the card. This further leads to people being misled by fake websites and emails.

Oman Khanleu (2009) has stated that the cases for misuse of ATM's are rising and this has increased the sense of insecurity among the people. This also needs to be taken under consideration so that the bank meets the expectations of its customers thereby building their trust over the online system.

Adeloye (2008) Concluded from his observation that security and power suspension were the major contributing factors for ATM frauds in Nigeria. Brunner et al. (2004) also stated one important factor that determines the safety of ATM is the location of the same. Research states that 75% of the ATM fraud cases is due to the isolated places of the ATM setups. Therefore ATM located near to banks is considered to be safer as compared to others.

Roli Bansal et al (2011) Keeping in view all the characteristics the minutia point features altogether with relative maps makes it easier to distinguish between the fingerprints. Further it was found that minutiae feature presentation is responsible to decrease the fingerprint pattern recognition.

The above part makes it clear that there have been large researches based on Bio-metric Protection system and much importance has been given to banks for security purpose. But to conclude hardly any type of research was there to explain

the need to make people aware. Therefore based on all this the study has been found.

III. RESEARCH METHODOLOGY & ANALYSIS

This section discusses the procedure and the logic employed for inspecting the operation of the Bio-Metric System. The domain of the study comprises Indian Scheduled Commercial Banking. Thus, for the sake of the present study, the Indian banking procedure was broadly classified into the two groups, namely an i.e. public (State Bank of Patiala, State Bank of India, CANARA Bank, Punjab National Bank and UCO Bank) and private (Axis Bank, HDFC Bank, Kotak Mahindra Bank, Yes Bank and ICICI Bank) sector bank in which five each banks was considered. Simple random technique was adopted to survey out the 500 respondents with drafted questionnaire.

The broader objective considered for the research study was to,

Degree of awareness among the employees of the banks about the implementation of the biometric system in the banks

Comparative analysis of the employees from the public and private sector banks about their awareness of the implementation of the biometric system in the banks

The respondents were surveyed on 5 – point likert scale regarding their general views on degree of implementation of biometric system. Respondents were surveyed on 7 different issues by asking questions like customers were satisfied with biometric banking, money matters are handled intelligently & efficiently with the system, the main system challenge is the safeguard of the security & privacy of customers, success of system depends upon the notch up security practices, need of the newer development of security parameters, banks needs to make that system strong, shortfall in authentication system and banks needs to adopt authenticated system for biometric. The analysis of the Table 1 showed respondents surveyed in the range of 72 – 75% were on the agreed range that customers were satisfied with biometric banking and money matters are handled intelligently & efficiently with the system. On the issues of authentications process still 52% of the respondents thought it is vulnerable while 29% respondents were against. Banks must offer strong authentication mechanism was being accepted by approximately 84% of the respondents surveyed. 92% of the respondents surveyed were of the view point that the main system challenge is the safeguard of the security & privacy of customers, and later approximately 74% respondents thinks that success of system depends upon the notch up security practices while 64% respondents surveyed were of the opinion that need of the newer development of security parameters and banks needs to make that system strong.

Table 1: Frequency Distribution Table of pattern of Responses on General Awareness regarding Degree of Implementation of Biometric System in Banking



H01: There was no significant difference between the average response scores of the respondents from both Public & Private sector banks.

Mann – Whitney Test (p – value)	0.401
------------------------------------	-------

	SA	A	N	D	DA
Online banking with biometric system helps in satisfying the banking needs of the client.	38.0%	37.5 %	16.5 %	5.2%	2.8%
Money can be managed intelligently and efficiently through online banking & biometric system	34.8%	37.0 %	15.5 %	8.8%	4.0%
The main challenge that the system faces is to safeguard the privacy and security of its customer's information	55.0%	37.2 %	3.0%	3.2%	1.5%
It can only succeed, if the security practices followed are top-notch	33.8%	40.5 %	11.8 %	7.8%	6.2%
Developing newer security technologies, is of paramount importance to keep the system safe and secure	25.0%	39.0 %	11.8 %	15.5%	8.8%
There are shortfalls, in the way in which authentication is done in system	27.2%	25.0 %	18.5 %	20.2%	9.0%
Ways adopted by banks to prove authenticity should be stronger	61.0%	23.5 %	13.2 %	2.2%	00%

The analysis of Table 2 showed there was no significant difference in average response score of the respondents from public and private sector banks on degree of implementation of biometric system in banks. Thus null hypothesis H03 was accepted (as all p – values were more than 0.05).

Table 4.14: Comparative Analysis of Average Response Score between Private & Public Sector Bank Respondents

Bank Sector		Degree of Implementation
Public	Mean	3.9
	Minimum	2.5
	Maximum	5.0
Private	Mean	3.9
	Minimum	3.1
	Maximum	5.0

IV. CONCLUSION

The purpose of the research paper was to analyze the awareness level among the employees belonging to the public and private sector banks about the implementation of the biometric system in the banks as they are the first one to know about the technicality pro and cons of the system. On comparison there was no difference in awareness level among employees of banks from both the sector and both sector employees demands for the better security measures for its effective implementation and also understand the easiness of the system in the future.

REFERENCES

- [1] Adeloye LA 2008. E-banking as new frontiers for banks. Sunday Punch, September 14, P. 25.
- [2] Byun S. and Buyn S. (2013) “Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters”. Behaviour and Information Technology, 32: 3, 217-230
- [3] Drygajlo, A., 2006. Information and communication security: Biometrics. Accessed 2014. Available at: <http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/01-Biometrics- Lecture-Part2-2006-10-23.pdf>
- [4] Ihejiashi R 2009. How to fight ATM fraud online. Nigeria Daily News, June 21, P. 18.
- [5] Jain, A., Arun A. Ross, A. and Karthik N. ,2011. Introduction to Biometrics. New York: Springer.
- [6] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 91-98.
- [7] Jain, A., Ross, A., Prabhakar, S., 2004. An introduction to biometric technology. Circuits and Systems for Video Technology, IEEE Transactions. Vol. 14, Issue 1. pp: 4-20.
- [8] Jain, A.K., Ross, A. and Pankanti, S. (2006), “Biometrics: A tool for information security”, Transactions on Information Forensics and Security, Vol. 1 No. 2, pp. 125-43.
- [9] James, T., Prim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the Technology Acceptance Model. Journal of Organizational and End-User Computing, 18(3), 1-24.
- [10] Lee (2006) How to Measure Survey Reliability and Validity. London: Sage.
- [11] Lee, D.T (2004): “Re-examining the security issues of ATM systems” Computer Fraud & Security 2004 Elsevier, pp. 13-15
- [12] Liao, S., Shao, Y., Wang, H., & Chen, A. (1999). The adoption of virtual banking: An empirical study. International Journal of Information Management 19, 63-74.
- [13] Litan, A. , 2004. Phishing Attack Victims Likely Targets for Identity Theft. Gartner Research.



- [14] Madu, C.N., & Madu, A.A. (2002). Dimensions of e-quality. *International Journal of Quality & Reliability Management*, 19(3), 246-58.
- [15] Margulis, S. (2011): "Three Theories of Privacy: An Overview" *Privacy Online – Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer Berlin Heidelberg, pp, 9-17
- [16] O’Gorman, L. Comparing Passwords, Tokens, and Biometrics for User authentication, *Proc. IEEE*, Vol. 91, No. 12, 2003, pp: 2021-2040
- [17] O’Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Paper presented at the *Proceedings of the IEEE*.
- [18] Obiano W 2009. How to fight ATM fraud. *online Nigeria Daily News*, June 21, P. 18
- [19] Omankhanlen Odidison (2009). ATM fraud rises: Nigerians groan in Nigeria. *Daily News*, Sunday, June 21, pp. 8-10.
- [20] Rhea, J (2002) "Army heads DOD biometric effort, defining system architecture with COTS" *Military and Aerospace Electronics* 13(11), pp: 3-5.
- [21] Roli, B., Priti S. and Punam B. (2011): Minutiae Extraction from Fingerprint Images. *International Journal of Computer Science Issues*, vol.8, Issue 5, No3. ISSN(online):1694-0814 www.IJCSI.org