ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

Awareness of Bio Metric System among Employees of 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 **-** Today's century is driven majorly by the IT scenario which has proved to be a great boon for the society but as every coin has two sides, hence the advancement in IT has urged the need to secure one's private database from the hackers. Therefore, today banks are scrolling for the techniques to provide quicker, easier and secured banking transactions to the authenticated users. Security is one major factor that holds the power to strengthen or disrupt the customer's trust in the banks. Implementation of an effective authentication method, that allows the access only to the authorized users, can contribute a great deal of help to the banks in providing safe and secured services to their customers. Thus, Biometric authentication method is one pioneer way that can be utilized in the banks in order to offer a relatively higher degree of security, which is implemented in numerous banks around the globe. One primary issue that arises while dealing with the application of the biometric authentication system at the banks is the consent of the employees and their willingness and flexibility to accept the change in the banking process. Therefore, the current paper discusses about the employees' conceptions with respect to the introduction and implementation of the secure biometric authentication system amongst the Indian public and private sector banks and the issue has been inspected vividly in the thesis.

I. INTRODUCTION

One significant factor that contributes to the growth and upliftment of an enterprise or organization is 'trust'. Hence, it is very vital for an organization to maintain a level of trust amongst its customers so as to maintain a healthy bond of client-customer relationship. Therefore, it becomes even more crucial for the financial institutions and banks to maintain a trustworthy bond as they hold a pivotal role in contributing towards the economic development of the countries. It is the primary objective of the banks specifically, to ensure that the customer's investments are in safe hands and are subject to no sort of danger. A bank can readily win the customer's reliance by maintaining pace, easiness and security in the services offered by the banks but there are other factors too which add to the process which compel the banks to take sufficient care of the customer's interests and hence leave no space for carelessness that may lead to security disaster. Being a part of this advanced IT world, the banks must take a step forward to adopt a security method which is both reliable and easy to use. Therefore, based on the analysis of the customers, the authentication process at the banks can be distributed into three broad categories:

Information that user knows (For instance- passphrase, PIN (Personal Identification Number))

Information that user owns (For instance- identification card, passport, swipe card, USB tokens and keys)

Information related to what user is (Biometric) (Wu, 1998).

II. BIOMETRIC SYSTEM

A biometric authentication system is designed to verify one's identity by measuring one or more physical or behavioral characteristics so as to provide access to the protected information only to the authorized users. Biometrics serve to be a secure and convenient authentication method since biometric traits are inherent to an individual, hence it offers complete protection as it is practically neither possible for the intruders to manipulate the biometric features nor for the users to share or forget their biometric characteristics (Jain et al, 2011). Some of the widely known techniques employed for biometric authentication include- hand scan, iris or retina scan, fingerprints, heart beat etc.

Biometric Technology has numerous applications in various aspects of daily life for instance- law enforcement, forensic applications, passport enquiry process, financial sector, industry employee registration, healthcare applications and many more to contribute to the list (Drygajlo, 2006). Thus, one is not wrong in saying that biometric technology offers a great deal of help in maintaining and uplifting the level of security for allowing authorized access only to the authenticated users. Specific major tasks that are involved in a banking system process include- branch banking, ATM banking, internet banking, telephone banking and POS banking. Therefore, the implementation of biometric protection system in these operations can bring a great advancement in the level of security. In addition to the benefits that the biometric protection technology showers on the bank organizations there are certain issues that require to be addressed with regard to the implementation of the biometric authentication system which includes- training of the employees, creating customer awareness, considering economical problems etc which are equally crucial and vital in the implementation process of a strong reliable protection system. The preliminary step that is required to be taken by the bank before initiating the process of implementation is to

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

evaluate and jot down the total cost that would be involved in the whole process of implementation of the biometric authentication system. Not to ignore that a robust reliable protection structure like Biometrics can prove to be advantageous if that banks are supported by knowledgeable employees who are quite familiar with the working of such a system and hence can contribute to the implementation process. The following sections throw some light on the advantages of the biometric authentication system.

III. USAGE OF BIOMETRIC SYSTEM

Banks hold the great responsibility of contributing to the country's economic power. With great responsibility comes the great power that the banks hold, making use of which they practice various financial policies with an eye to uplift the current level of economic growth of the country. However, there may also occur a situation where the financial policies implemented by the banks may lead to an economic slowdown in the country. As per the utmost vital status of the banks and the other financial institutions, the issue of security holds greater priority in this sector of industry. Information which is the useful, meaningful and the confidential piece of data is preserved under the supervision of an organization for the interests of the customers, therefore it becomes the crucial responsibility of the enterprise to make sure that the promises made to the customers with regard to the protection of their private information is kept and obeyed. The banks must take the initiative of safeguarding the information from any kind of unauthorized access by an intruder. By increasing identity theft, legislators are encouraging banks to elevate the status of their authentication systems, however still many banks are utilizing the obsolete protection systems which are not updated enough to prevent the intruders from attacking (Litan, 2004). It is quite obvious from the fact that the absolute identification of an individual can contribute a lot in eradicating the cases of theft and fraud in banks (Jain et al, 2011) hence the banks must sincerely lay stress on the employment of a strong updated authentication system.

IV. ADVANTAGES OF BIOMETRIC SYSTEM

Today, the traditional authentication methods which involved the usage of passwords and tokens do not guarantee enough security due to the increasing level of intruder attacks. As per (O'Gorman, 2003), there are different kinds of attacks (Trojan Horse, Replay Attack, Host Attack, Phishing Attack, Brute Force Attack, Eavesdropping, Host Attack, Denial of Service etc) prevalent against the protection systems relying on passwords and tokens. Comparatively, biometrics offer stronger level of protection system safeguarding the interests of the clients/customers since an intruder or a hacker cannot play with the biometric traits unlike the passwords and tokens. In addition biometrics serve to be a best option as user-friendly, convenient authentication systems since they relieve the users from the overhead burden of remembering the complex passwords, user Ids or Login Ids, transaction Ids etc (Jain et al, 2004).

V. LITERATURE REVIEW

In today's scenario where internet has touched almost every aspect of life, it becomes very crucial to secure the information traversing through the web. Therefore, in order to promote internet banking amongst the customers it is very vital to ensure that the security measures undertaken do not compromise with the privacy rights of the customers, Peterson (2003). According to the study conducted by Lee (2006), a new scenario came into picture which revealed that the acceptance rate of the facility of online banking is influenced majorly by demographic factors, it was further revealed that the section of population which utilizes this facility the most points towards the youth, who use this facility for numerous online transactions permitted by the banks (like online shopping of various products e.g. clothes, food etc).

As per the views of David (2006), the success of an e-banking facility relies to a great extent on the financial products and the quality of service offered to listen to and satisfy to the needs of the customers. Further, David (2006) also discussed that certain factors like convenience and easiness in using the banking system, assurance of secure transactions and the pace of the network are some of the characteristic features which effect the utilization of online banking concept amongst the customers.

The decision of the customer to prefer online banking depends on the single most vital factor which includes the vivid research on the customer relationship management, David (2008).

Boukhonine et al., (2005), the fundamental objective of a bank is to offer a sound environment of protection to its customers in internet banking transactions. The factors that hold a great potential role in the process of framing a reliable security policy include accountability, integrity, confidentiality, availability and non-repudiation concerns. Thus, the banks employ a robust security policy by keeping in focus the above discussed potential concerns by utilizing various physical devices like support access cards, and automated monitoring system that holds the right to accept or reject the deployment or usage of any particular information or object into the system.

Madu and Madu (2002) were of the view that security of the private information of the customers is the major cause of dissatisfaction among them as they are not sure about the reliability of the authentication system being used by the banks.

Ihejiahi (2009) expressed his concern about the issue of increasing cases of ATM frauds in the market and the banks failing to address the soaring issue with sincerity. He was of the view that the banks which are supposed to be the most reliable and trustworthy organization for the customers must deploy such a protection method which envelops a strong firewall against such online theft cases.

Obiano (2009) was of the view that the task involving distribution of ATM cards among the customers was done without creating proper awareness and knowledge about the utilization of the card, due to which the customers generally exhibit careless attitude in maintaining the crucial card details like PIN number properly and also get easily deceived by the

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

various fake websites and text messages demanding the card details of the customers.

Omankhanleu (2009) has put forth an opinion that the soaring situations of ATM (Automated Teller Machine) fraud cases are piling up to the issue of customer dissatisfaction which requires great attention and thought from the banks' perspectives of the nation so as to keep up to the expectations of the customers and allow them a safer sound journey in pursuing online transactions.

Adeloye (2008) observed that the major factors which contributed to the ATM fraud cases in Nigeria were security and power suspension. Further, Brunner et al. (2004) concluded in their study that one vital factor responsible for ATM thefts is possibly the location of the ATM point. The facts fetched from the research showed that about 75% of the ATM swindle cases, as asked by respondents, were due to the deserted locations of the ATM points. Thus, an ATM point located at a nearby spot to the banks is supposed to have relatively more security in comparison to the one located in a secluded place, hence a place of crowd like malls, market place etc can serve to be the most suitable locations for the ATM points where chances of thefts are negligible.

Diebold (2002) stated that a major proportion of ATM fraud cases occurred as PIN theft i.e. stealing away of the PIN number of an ATM holder. It was reported that majority of the customers were struck by PIN thefts, which occurs mainly by shoulder surfing, keypad recording equipment, skimming etc. On further research it came out that PIN thefts occur majorly due to congestion at the ATM points, an issue to be addressed and sorted. Certain other forms of ATM fraud cases that came on bench from the respondents included card theft, force withdrawal etc at the ATM point. Thus, it came out that the protection at ATM points, say by appointing a guard was essential.

Cynthia (2000) presented a view that providing ATM service round the clock is like two sides of a coin situation, which has both the bright and the dark side.

Roli Bansal et al (2011) addressed that keeping in consideration all the fingerprint features, the minutia point characteristics clubbed with relative orientation maps are quite exclusive to distinguish amongst the fingerprints effectively. It was further stated that the minutiae feature presentation contributes a lot in reducing the intricate fingerprint pattern recognition to a point pattern matching query.

It is quite clear from the above discussed and portrayed literature review that numerous studies have organized and observed with regard to Bio-Metric Protection System specifically with respect to banks keeping in view their security perspectives. However, it was observed that rarely any sort of research was conducted to illustrate the urgency of awareness creation to the bank customers and employees. Thus, on the basis of the above discussion, the following study was proposed. Following comprise the definitive objectives of the current study,

To appraise the rate of effectuation of the Bio Metric Systems in the Banks

To appraise the performance and the efficacy of the Bio Metric Systems implemented in the Banks

To appraise the views and aspects of the Bank employees' perspective with regard to the Bio Metric System

To seek ideas or suggestions for the efficient deployment of the advanced Bio Metric Authentication System in the Banks.

VI. RESEARCH METHODOLOGY

Effectuation, efficiency and evaluation of the perception of the employees in relation with the implementation of the Bio Metric System in the Indian banks, comprises the basis of the present research study. The study imparts an elaborate vivid description about the utilization of the robust Bio-Metric Authentication system in the banks.

SAMPLE DESIGN AND SAMPLE UNIT

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 following groups, namely:

Group I- Public Sector Banks (5 Banks)

Group II- Private Sector Banks (5 Banks)

The banks that shall be focused upon in the present study under the category of public sector banks shall include State Bank of Patiala, State Bank of India, CANARA Bank, Punjab National Bank and UCO Bank.

The banks that shall be focused upon in the present study under the category of private sector banks shall include Axis Bank, HDFC Bank, Kotak Mahindra Bank, Co – Operative Bank, Yes Bank and ICICI Bank.

Since the effectiveness of a system can be well examined and improved only if one is aware with the perspectives of the individuals who drive the system, hence to conduct the research study and to further record and evaluate the views of the bank employees with respect to the implementation of a stronger security system like Biometrics about 500 bank employees will be selected comprising 50 from each individual bank. The bank employees who would be interviewed would include primarily the clerks, front line managers, cashiers, accountants etc, people who are in direct contact with the authentication system and hence their views can resort to be valuable. Thereafter the elected respondents will be presented with a set of framed questionnaire and their responses will be measured on a five-point psychometric scale i.e. Likert scale.

VII. DATA SOURCE

For the current study the data deployed will be accumulated from both the fieldwork as well as the paperwork. The fundamental data that will hold the power to influence the conclusion would be the information fetched from the respondents via well framed questionnaire. Further, a pilot study in the region of North India will also be pursued so as to ensure the flexibility and extensibility of the responses collected via questionnaire. The questionnaire will be drafted by keeping in focus the objectives of the research study and the structure of questionnaire will be in direct congruence with the present research literature and the discussions held

with the banking personnel, bank customers and the respective academicians. However, wherever required the secondary data may also be deployed to complete the present research study.

VIII. 8. CONCLUSION

It is quite clear from the above discussed and portrayed literature review that numerous studies have organized and observed with regard to Bio-Metric Protection System specifically with respect to banks keeping in view their security perspectives and also imparts an elaborate vivid description about the utilization of the robust Bio-Metric Authentication system in the banks. It is analyzed using the appropriate data, the data which is collected from the Indian banking procedure was broadly classified into the two groups to solve complex problems like related using Data mining techniques.

REFERENCE

[1] Adeloye LA 2008. E-banking as new frontiers for banks. Sunday Punch, September 14, P. 25.
[2] Brunner, A., Decressin, J. and Kudela, B. (2004): Germany's Three-Pillar Banking System – Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC.
[3] Cynthia B. (2000). The measurement of white-collar crime using Uniform Crime Reporting (UCR) Data. S department of Justice, Federal Bureau of Investigation, New York.
[4] Diebold I. (2002). ATM fraud and security: White Paper, New York.
[5] 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
[6] Ihejiahi R 2009. How to fight ATM fraud online. Nigeria Daily News, June 21, P. 18.
[7] Jain, A., Arun A. Ross, A. and Karthik N. ,2011. Introduction to Biometrics. New York: Springer.
[8] 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.
[9] Lee (2006) How to Measure Survey Reliability and Validity. London: Sage.
[10] Litan, A. , 2004. Phishing Attack Victims Likely Targets for Identity Theft. Gartner Reasearch.
[11] Madu, C.N., & Madu, A.A. (2002). Dimensions of e-quality. International Journal of Quality & Reliability Management, 19(3), 246-58.
[12] O'Gorman, L. Comparing Passwords, Tokens, and Biometrics for User authentication, Proc. IEEE, Vol. 91, No. 12, 2003, pp: 2021-2040
[13] Obiano W 2009. How to fight ATM fraud. online Nigeria Daily News, June 21, P. 18
[14] Omankhanlen Odidison (2009).ATM fraud rises: Nigerians groan in Nigeria. Daily News,Sunday, June 21, pp. 8-10.
[15] 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
[16] Wu, Th., 1998. The secure remote password protocol. In proceeding of the Internet Society Network and Distributed System Security Symposium, pp 97-111.

