Inspira- Journal of Modern Management & Entrepreneurship (JMME)
ISSN : 2231–167X, General Impact Factor : 2.7282, Volume 09, No. 02, April, 2019, pp. 73-83

ANALYTICAL STUDY ON THE IMPACT OF BIOMETRIC SYSTEMS IN BANKING SECTOR

Dr. S.Saravanan*
DR. S.Velayutham**

ABSTRACT

The word biometric can be defined as "life - measure." It is used in security and access control applications to mean measurable physical characteristics of a person that can be checked on an automated basis. Although you may not think about it, your driver's license contains biometric information about you. Your height, weight, hair color and eye color are all physical characteristics that can easily be checked. However, your height changes with age (16 years old drivers get taller, senior citizens get shorter). Your hair color changes naturally (and on purpose). You can wear colored contact lenses that change your eye color; everyone's weight fluctuates over time. Biometrics-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., Speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens. Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges (e.g., key, password) of a genuine user and the genuine user himself/herself. Furthermore, biometric authentication systems can be more convenient for the users since there is no password to remember or key to protect and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords. Although biometrics emerged from its extensive use in law enforcement to identify criminals (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, forensics, positive identification of convicts and prisoners), it is being increasingly used today to establish user recognition in a large number of civilian applications.

KEYWORDS: *Bio Metric, ATM Users, IT People, Fingerprints, Identify Criminals.*

———————————

Introduction

Biometrics-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., Speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens. Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges (e.g., key, password) of a genuine user and the genuine user herself. Furthermore, biometric authentication systems can be more convenient for the users since there is no password to be forgotten or key to be lost and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords.

* Assistant Professor, PG and Reasearch Department of Commerce, Dr. Ambedkar Government Arts College, Vyasarpadi, Chennai, Tamilnadu, India.

** Assistant Professor, Department of Business Administration, Mohamed Sathak College of Arts and Science, Sholinganallur, Chennai, Tamilnadu, India.

What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- **Universality:** each person should have the characteristic;
- **Distinctiveness:** any two persons should be sufficiently different in terms of the characteristic;
- **Permanence:** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- **Collectability:** the characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:

- **Performance**, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- **Acceptability**, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- **Circumvention**, which reflects how easily the system can be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

Identified Problem

Identity theft is the fastest growing crime in the India – affecting more than 100,000 people across, according to Home Office figures. This could also be the problem for any country which has technological developments across. Most common problems heard in banking sectors across globe are:

- Card cloning
- Pin thefts

A survey conducted by Fujitsu four years ago found that one in three banking customers is ready to embrace biometric technologies in the hope of adding greater security to their finances.

- **Data Losses**: Recent high profile cases of sensitive data being lost by financial and also public sector organizations has highlighted the risk to individuals and to the reputation of the organizations concerned. People lose their data either on online trading or any bogus or phishing websites.
- **In Conjunction with Police Department:** The Biometric data can be verified with the police department to identify any criminals having an account and trying to access any banking solutions.

Need for Study

- To help ease/secure the application access to the nescient, aged and challenged people
- To secure all the banking applications with at most care
- To protect all the banking clients with secure gateways
- A stepping into the implementation of latest technologies
- To overcome the problems from hackers, by theft of passwords and fraudulence
- To overcome the problems of carrying cards everywhere you go.

Objectives of the Study

- To analyze the impact of biometric systems in banking solutions
- To conclude the best fit approach for the next generation banking
- To analyze, on whether people welcome this biometric systems to be implemented in all operations
- To analyze, on FMR and FNMR errors in biometric systems
- To analyze, the peoples satisfaction level on usage of this biometric systems

Scope of the Study

- To analyze with survey from public on the trends in banking solutions with respect to biometrics implementations
- To analyze the best fit approach for banking transactions
- To collect/generate views concerning potential biometrics implementations in banking solutions
- To study the verification and Identification strategies

Methodology

- Is a way to systematically solve the research problem.
- It may be understood as a science of studying how research is done scientifically.
- The research methodology in the present study deals with research design, data collection methods, sampling methods, survey, analysis and interpretation and limitations of the study.

Target Respondents

- Professionals from banking sector
- Financial Institutions
- Industrialists
- Research professionals
- Individuals from various domains, wants to implement biometric systems
- Student

Sampling Methods

From the population the researcher took the sample size of 100.

Data Processing/Collection

- **Primary Data**

Primary data was collected either through online forums or through direct communication with respondent in one form or another. The primary data was collected, through structured questionnaire which is given in the annexure.

- **Secondary Data**

Secondary Data means data that are already available i.e., they refer to the data which have already been collected and analyzed by someone else. The secondary data was used to support primary data. Company report, websites, magazines were widely used.

Tools for Analysis

The statistical tools and test used for this study are.

- Simple Percentage analysis.
- Weighted Average Analysis.

Data Analysis and Interpretation

The data for this study has been collected through the structured questionnaire from a population (Bio metric ATM users, IT people having knowledge about bio metrics and residents who work in Biometric ATM's) the help of various statistical tools which includes Percentage Analysis and Weighted Average Method and then study the results according to the objectives formulated at the beginning of the study.

Table No	Questionnaire	Very Low	Low	Nominal	High	Very High	Total
1	Do you have sufficient knowledge on the functionality of how the Biometric system is working and how to escalate if any issue occurs?	21	34	23	16	6	100
2	Do you have awareness on the places where this system is located in your city?	12	20	31	24	13	100
3	How complex is the current biometric system?	36	27	21	13	3	100

4	What is the frequency of transaction through biometric ATM?	6	14	61	17	2	100
5	Have you faced any difficulty in placing the fingerprint while hurt or other miscellaneous accidents in finger and accessing the system.	94	4	1	0	1	100
6	If so, you like the system, in how many operations you would like to implement.	4	21	8	28	39	100
7	What is the extent of the Biometric banking on ATM centers are expected to perform its intended functions satisfactorily (reliability required)?	44	37	19	0	0	100
8	What are the expected execution time / processing time of the biometric ATM centers?	24	34	26	12	4	100
9	How convenient is the biometric system compared to the legacy card holding transaction. Provide your convenience level as 1- less convenient and 5 – highly convenient.	22	27	32	13	6	100
10	What is the level of non volatility of the biometric systems installed in the ATM centers with respect to accessibility level?	0	0	0	9	91	100
11	How often solutions for errors occur in the system FMR(False match rate) and FNMR(False non match rate)	1	5	19	30	45	100
12	What is the experience with the hardware and software configurations of the biometric systems in ATM centers?	11	19	15	39	16	100
13	What is the degree you welcome this biometric systems in banking solutions	5	6	21	27	41	100
14	What is the degree of recommendation with the hardware and software configurations of the biometric systems in ATM centers?	12	18	18	36	16	100
15	What are the suggestions or enhancements to be implemented in the future releases of the software or hardware upgrade.	To be considered for conclusion					

Data collected are shown below in the form of tables and charts:

Simple Percentage Analysis

Chart 1

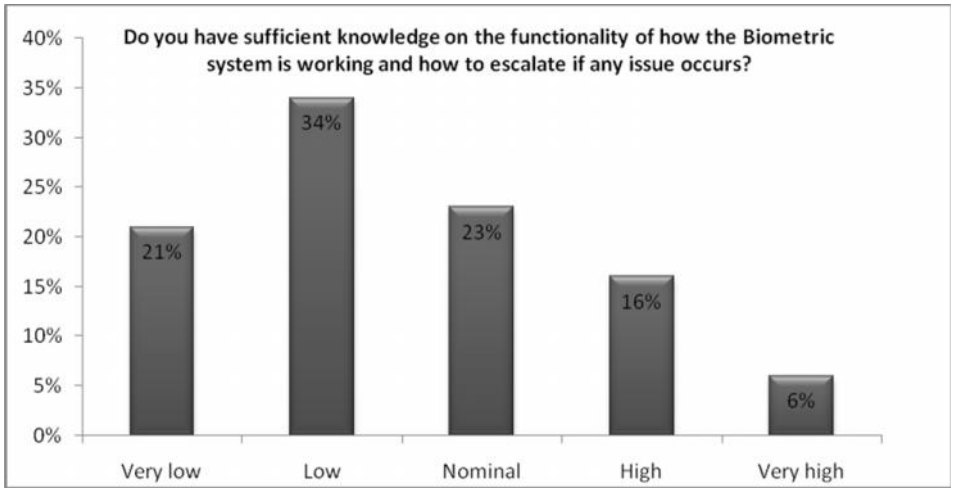


Chart 2

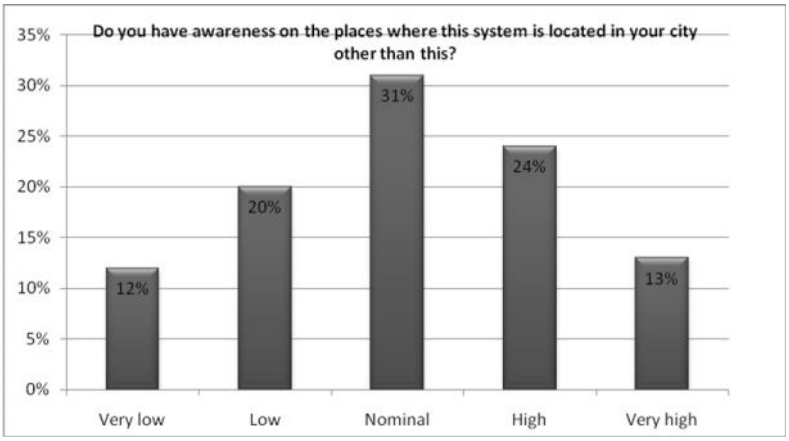


Chart 3

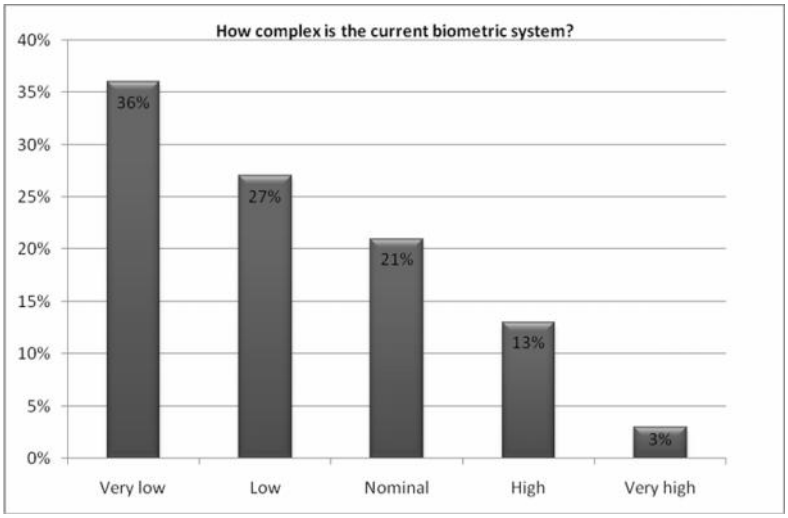


Chart 4

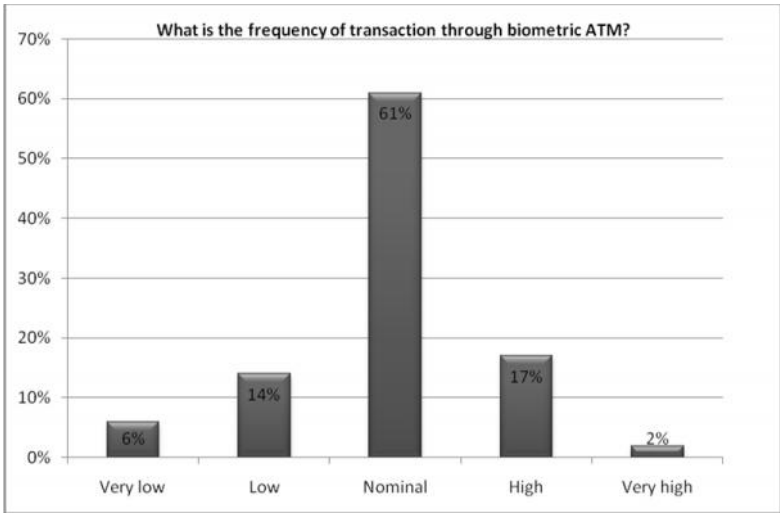


Chart 5

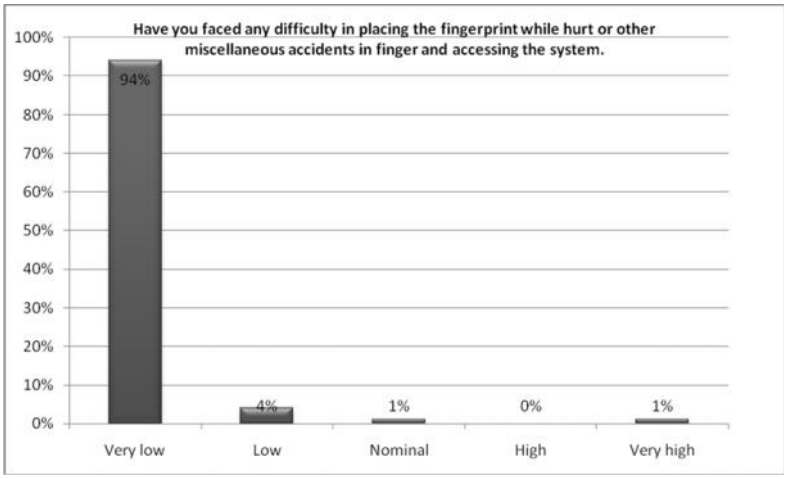


Chart 6

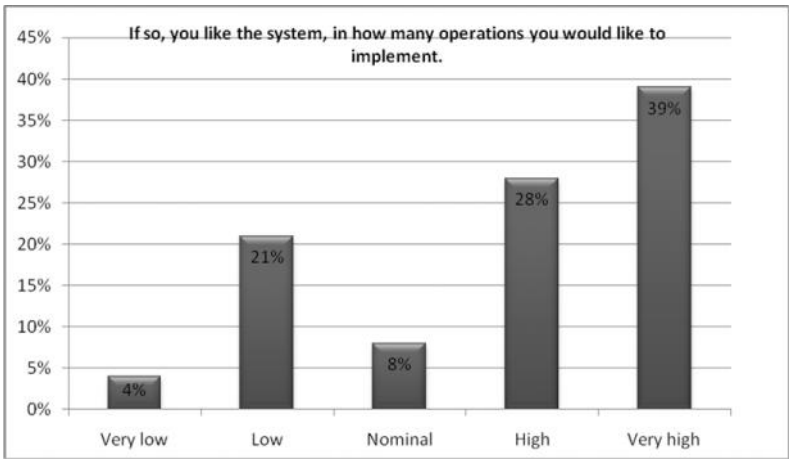


Chart 7

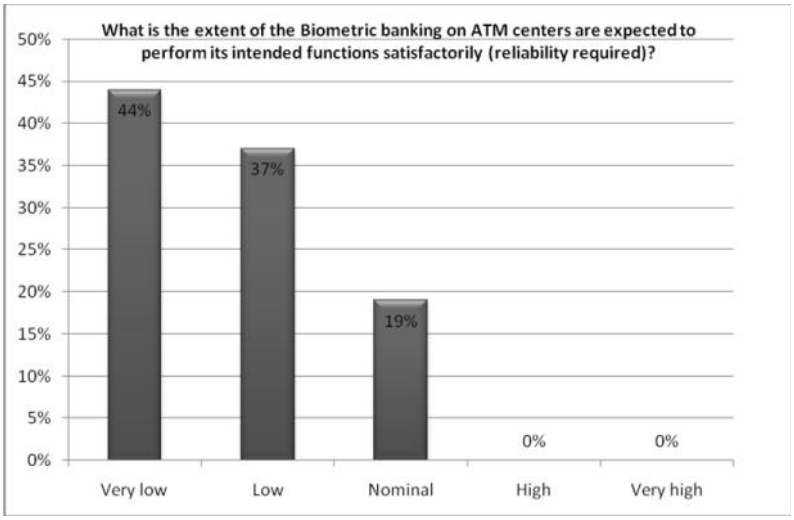


Chart 8

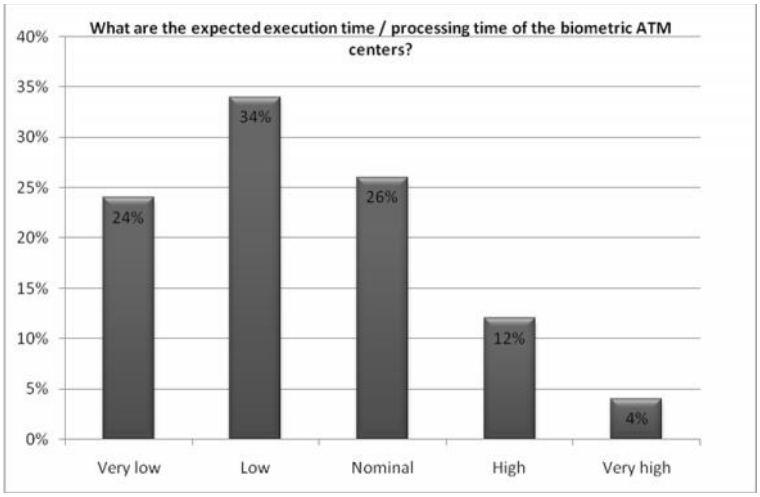


Chart 9

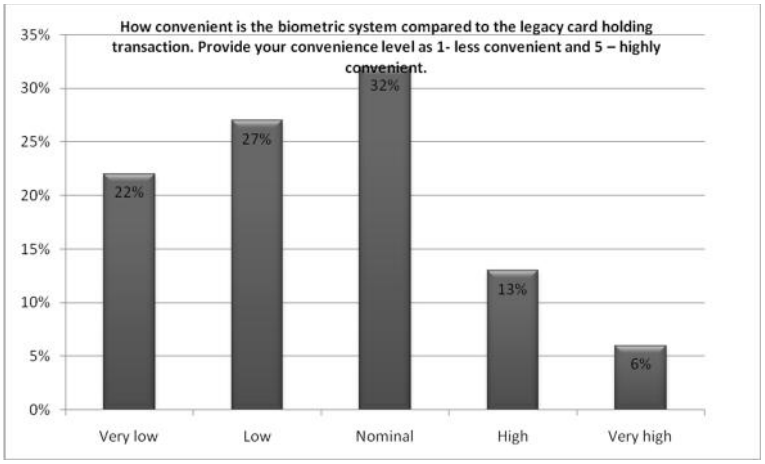


Chart 10

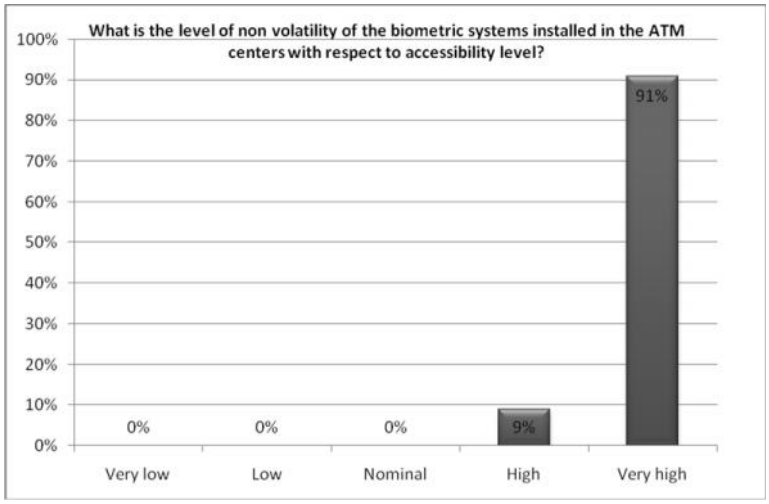


Chart 11

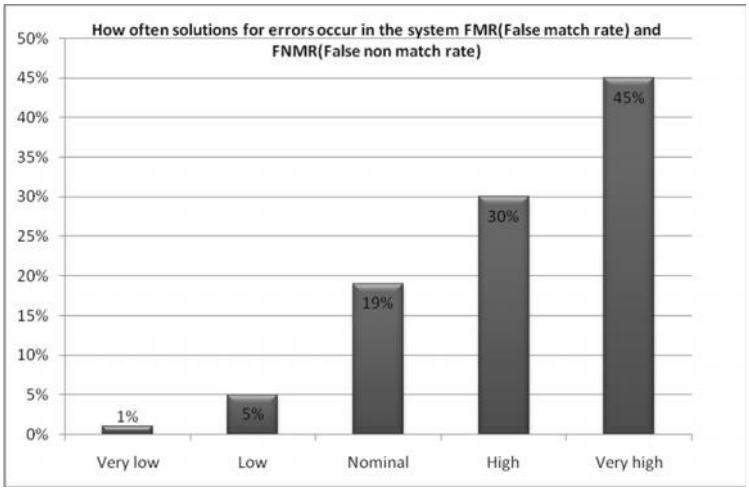


Chart 12

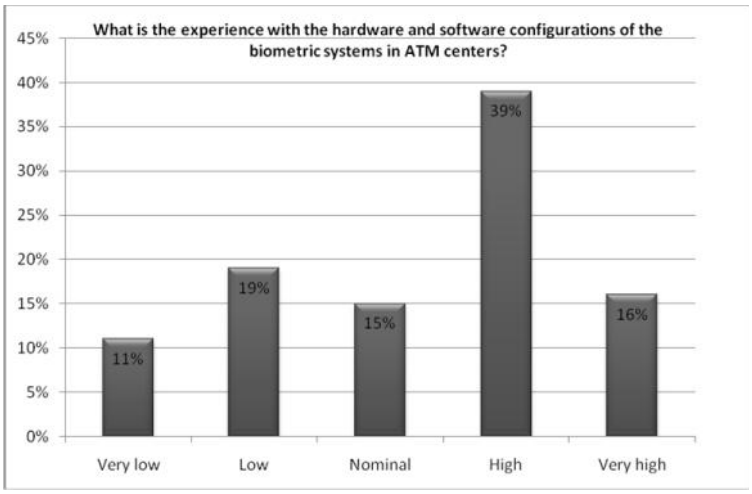


Chart 13

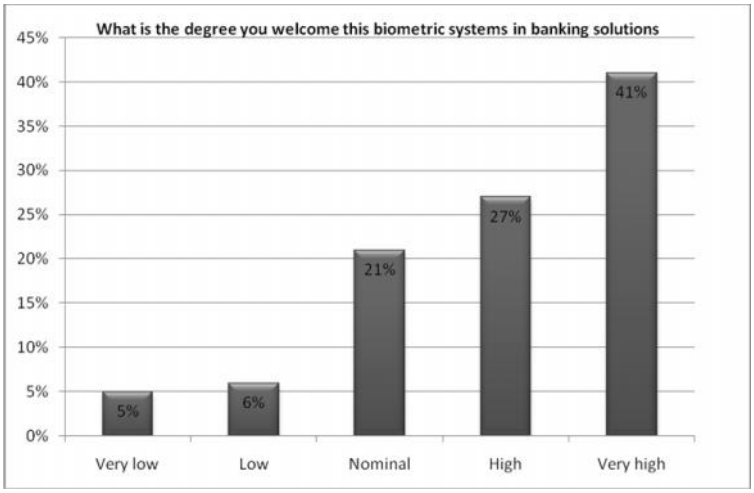
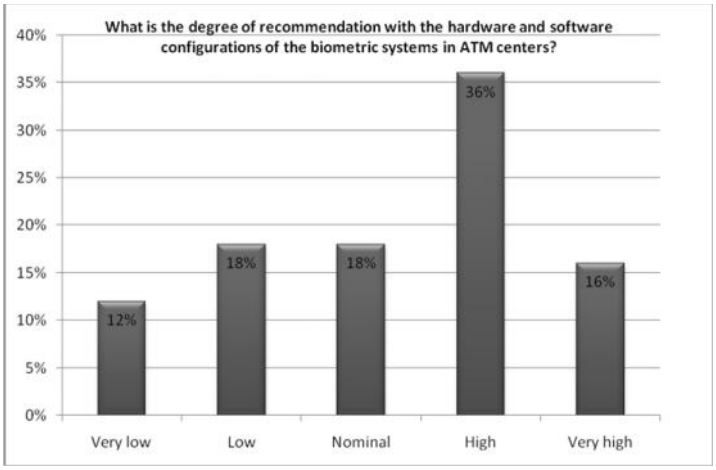


Chart 14



Weighted Average Analysis

T. No.	Questionnaire		Very Low	Low	Nominal	High	Very High	Total
9	How convenient is the biometric system compared to the legacy card holding transaction. Provide your convenience level as 1- less convenient and 5 – highly convenient.		22	27	32	13	6	100
	The convenience level is given as 1-5 hence Xi is:		1	2	3	4	5	
	And now the weightage given by people Wi is:		22	27	32	13	6	
	And the formula ∑ Wi * Xi =		22	54	96	52	30	254

How convenient is the biometric system compared to the legacy card holding transaction. Provide your convenience level as 1- less convenient and 5 – highly convenient.

- Very Low
- Low
- Nominal
- High
- Very High

Let the weighted mean be ∑Wi = 100 (samples taken), And now calculating Weighted average mean to be (∑ Wi * Xi) / (∑Wi) = 2.54 (Calculated)

Inference

Hence the value comes to be greater than 50% ie 2.54

Conclusion

Thus, people who use the system are highly convenient towards the usage of the system.

Summary of Findings

- People are yet to gain more knowledge about the systems functionality and how it is being applied and how to troubleshoot if any problem occurs.
- people tend to know their nearby ATMs and would like to do frequent transactions on those well known ATMs only.
- people tend to get more support at very initial stage and subsequent to that, they try this system by themselves

- Thus people tend to use this system at a normal rate of 1-5 transaction and this is the average compared to the usage of the traditional way of using the system.
- Thus, most of people have never met this type of situation so far and very few have faced and the result of inference cannot be accurate
- Thus, from the inference chart, most of people would like this kind of system to be implemented across all the banking operations.
- People does not face software problems and the recovery of their money is simple and ease
- People face the processing time is much better and their procedure of access is little complex\
- Thus, people feel more convenient and satisfactory by the usage of this sort of biometric systems compared to the legacy card holding systems
- Thus, people feel, there is not much difference while on initial stage to till date
- People feel, there are no FMR and FNMR issues and they have never come across these sorts of issue faced by others till now
- People feel the hardware and software configurations of the systems are same and not much difference.
- People welcome this sort of biometric ATMs to be implemented in all the banking operations
- Thus, the peoples approach towards software and hardware configuration is OK and they require little user friendliness.
- Thus, the people prefer to opt for safe and secure way of transactions. Hence people opt for their transaction through biometrics
- Thus, the people wish to implement this Biometric system ATM in all the banks. People opt this way of transaction the most convenient way of banking
- Thus, the user satisfaction levels of biometric ATMs are high and acceptable as per the assumptions. People satisfactory level is more in this type of ATMs
- Thus, the occurrences of error in this kind of biometric ATMs are very minimal. People feel that these ATMs are error free.
- Thus, people welcome this sort of biometric systems to be implemented across all the functional areas. People welcome this type of biometric ATMs
- Thus, people who use this system feel that this is highly convenient.

Suggesions and Recommendations

Biometrics refers to an automatic recognition of a person based on his/her behavioral and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics does bring an increase in security, will it be worth the financial cost? Hence the cost of implementing these systems across all ATMs should be minimized. This system may be extended to all applications where identity checks are essential such as authorized entry, access etc., related to defense, research, confidential data , sensitive information's etc

Conclusion

After analyzing the feasibility of attacks against fingerprint-based biometric systems, we have shown that the proposed attacking system is quite effective when breaking into accounts protected with templates composed of minutiae location and angle information. The system was able to synthesize templates that guarantee positive identification in a relatively small number of attempts (271 on the average). Even though we proposed several measures to counter such attacks, each has its own limitations, especially for multimodal biometric systems. We are currently working on modified attack systems with the aim of decreasing the number of attempts even further.Thus the biometric systems are welcome by majority of users who actually use this system and hence this type of operations should be

implemented across all banking solutions for global applications for efficient access tracking and ease of operations. Finally, the use of biometrics raises several privacy questions. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation. For example, if and when face recognition technology improves to the point where surveillance cameras can routinely recognize individuals, privacy, as it has existed in the public sphere, will be wiped out. Even today, in some major cities, you are recorded approximately 60 times during the day by various surveillance cameras. In spite of all this it is certain that biometric-based recognition will have a great influence on the way we conduct our daily business in near future.

References

- A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
- B. Schneier, “The uses and abuses of biometrics”, Comm. ACM, vol. 42, no. 8, pp. 136, Aug. 1999.
- D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.
- N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
- R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners”, Pattern Recognition, vol. 36, pp. 383-396, 2003.
- T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of Artificial Gummy Fingers on Fingerprint Systems”, Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275-289, 2002.

♦❒♦