INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

as well as in Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)]

Registered & Listed at: Index Copernicus Publishers Panel, Poland

Circulated all over the world & Google has verified that scholars of more than 1500 Cities in 141 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

www.ijrcm.org.in

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, KurukshetraUniversity, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

ANALYTICAL STUDY ON BIOMETRIC SECURITY APPLICATION IN INDUSTRIAL AND MOBILE BANKING SECTOR

DR. U. S. PANDEY
ASSOCIATE PROFESSOR
SCHOOL OF OPEN LEARNING
DELHI UNIVERSITY
DELHI

GEETANJALI GUPTA
RESEARCH SCHOLAR
SINGHANIA UNIVERSITY
PACHERI BARI

ABSTRACT

The aim is to enable users to exchange information that can not be disputed afterward. That could be a voice recording that is authenticated to eliminate any doubt that the speaker is what they actually said and prove that it has not been manipulated. To achieve this it is necessary to digitally sign the data and to ensure only the legitimate user can perform the signing. At present, security for mobile banking transactions rests on several parallel approaches: device-based security, such as the unique SIM card within each mobile handset that identifies the customer who owns the phone; know-your-customer requirements and establish their identity to the bank in order to open the account. The weakest link is device-base security. In order to do so, countries need to pursue both broader coverage of cellular networks, and better connectivity in the form of affordable mobile phones and easier access to financial and other types of services. For the banking sector to provide financial services in rural areas, the issues they face include not just coverage and connectivity, but also basic familiarity with banking systems, from training and education in the use of bank accounts to the provision of adequate security measures for users unfamiliar with Pins and passwords and who often have few formal identification documents. It is the security issue that is of particular importance to financial institutions, not just in developing countries but worldwide, led by growing concerns about money laundering and terrorist financing, fraud and consumer protection. An area of rapid development in security systems is the use of biometrics. While fingerprints have long been used in law enforcement, other types of biometrics have largely been the stuff of research and science fiction. As technology improves, the ability to use biometrics for individual applications, particularly in mobile banking, is of great interest to financial institutions seeking secure means of signing up rural customers.

KEYWORDS
Biometric security, mobile banking.

1.1 INTRODUCTION

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain *et al.* (1999) *[1].* identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication **Universality** means that every person using a system should possess the trait. **Uniqueness** means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. **Permanence** relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. **Measurability** (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. **Performance** relates to the accuracy, speed, and robustness of technology used. **Acceptability** relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. **Circumvention** relates to the ease with which a trait might be imitated using an artifact or substitute.

A biometric system can operate in the following two modes. In **verification** mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity".

In **Identification** mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be" The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective EITO *[2].*

The first time an individual uses a biometric system is called *enrollment*. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area)

2.0 OBJECTIVES

PRIMARY OBJECTIVE

The aim is to enable users to exchange information that can not be disputed afterward. That could be a voice recording that is authenticated to eliminate any doubt that the speaker is what they actually said and prove that it has not been manipulated. To achieve this it is necessary to digitally sign the data and to

ensure only the legitimate user can perform the signing. At present, security for mobile banking transactions rests on several parallel approaches: device-based security, such as the unique SIM card within each mobile handset that identifies the customer who owns the phone; know-your-customer requirements, especially for the retail cash-in/cash-out points that are usually required to have a traditional bank account and establish their identity to the bank in order to open the account. The weakest link is device-base security. In order to do so, countries need to pursue both broader coverage of cellular networks, and better connectivity in the form of affordable mobile phones and easier access to financial and other types of services. The economics of extending high-cost cellular networks into rural areas cannot usually be justified without high voice and data traffic forecasts beyond basic coverage, however, is the need to link users to useful financial services via easy-to-use handsets and simple applications N.K.Ratha*[3].* For the banking sector to provide financial services in rural areas, the issues they face include not just coverage and connectivity, but also basic familiarity with banking systems, from training and education in the use of bank accounts to the provision of adequate security measures for users unfamiliar with Pins and passwords and who often have few formal identification documents. It is the security issue that is of particular importance to financial institutions, not just in developing countries but worldwide, led by growing concerns about money laundering and terrorist financing, fraud and consumer protection. An area of rapid development in security systems is the use of biometrics. While fingerprints have long been used in law enforcement, other types of biometrics have largely been the stuff of research and science fiction. However, rapid advances in biometric technology, largely driven by national security concerns, have brought several biometric solutions to the market, especially for border control, physical access and fraud prevention. To date these biometric systems have largely been complex and expensive to build and operate, and have thus been limited in their implementation. As technology improves, the ability to use biometrics for individual applications, particularly in mobile banking, is of great interest to financial institutions seeking secure means of signing up rural customers.

MAIN OBJECTIVES OF THIS STUDY

As today scenario many changes and crimes happened in every sector, we see many frauds in every sector just like misuse of credit and debit cards, wrong identity and most wrong customer description so all these frauds created by only one reason that is no sound details about the consumer. In said research we find out those ways and methods which create more effective data record for bank and describe how biometric instrument help in this process. Some specified objectives are-

- To identify the need and reasons behind of using biometric security system.
- Giving details about security equipment which useful in banking and industrial sector.
- Identify the importance of these security and how much these useful in organization.
- Identify all perquisites about the security system in organization and what's technique using prefer in the organization.

3.0 SCOPE OF RESEARCH

With the growth of Modern Era, People started showing more interest in ATM Banking, etc. Biometric is a speedy and efficient mode of identifying the valid user. Not limited to general application, Biometric is also used for security measures such as identifying terrorist who never believes in holding password and always carry fake Smart cards etc. To prevent identity theft, biometric data is usually encrypted when it's gathered. Here's how biometric verification works on the back end: To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied.

It is certain that fingerprint sensors will be central in new phone offerings. Consumers will need this new approach to security to handle the high-speed access that cell phones will provide. Cell phones will act as debit and credit devices. The practice of swiping an ATM card or a credit card at the supermarket is already established. Putting that same technology into a cell phone's SIM card is the next logical step. There is evidence of that trend already developing in foreign markets. In Japan, workers use cell phones for keyless entry. Train stations have devices that read the cell phone data chip to make a ticket purchase, rather than using a debit card. In South Korea, consumers are able to conduct online banking transactions from their mobile phones much the way they do from their desktop computers. M-Commerce from cell phones will be one of the next big advancements in consumer convenience Iuarn[*10].* Consumers will not only be able to order tickets and make seat selections with their cell phones; they will download the ticket into their cell phone's memory and use that data to enter the theater.

4.0 LITERATURE REVIEW

COUNTRIES APPLYING BIOMETRICS

AUSTRALIA

Visitors intending to visit Australia may soon have to submit to biometric authentication as part of the Smart gate system, linking individuals to their visas and passports. Biometric data are already collected from some visa applicants by Immigration. Australia is the first country to introduce a Biometrics Privacy Code, which is established and administered by the Biometrics Institute. The Biometrics Institute Privacy Code Biometrics Institute forms part of Australian privacy legislation Gefen *[8]*. The Code includes privacy standards that are at least equivalent to the Australian National Privacy Principles (NPPs) in the Privacy Act and also incorporates higher standards of privacy protection in relation to certain acts and practices. Only members of the Biometrics Institute are eligible to subscribe to this Code. Biometrics Institute membership, and thus subscription to this Code, is voluntary.

BRAZIL

Since the beginning of the 20th century, Brazilian citizens have had user ID cards. Each state in Brazil is allowed to print its own ID card, but the layout and data are the same for all of them. The ID cards printed in Rio de Janeiro are fully digitized using a 2D bar code with information which can be matched against its owner off-line. The 2D bar code encodes a color photo, a signature, two fingerprints, and other citizen data. This technology was developed in 2000 in order to enhance the safety of the Brazilian ID cards Wang*[9]*.

CANADA

Canada has begun research into the use of biometric technology in the area of border security and immigration (Center for Security Sciences, Public Security Technical Program, and Biometrics Community of Practice). At least one program, the NEXUS program operated jointly by the Canada Border Services Agency and U.S. Customs and Border Protection, is already operational. Friedman*[7]* It is a functioning example of biometric technology, specifically "iris recognition biometric technology"[16] used for border control and security for air travelers.

GERMANY

The biometrics market in Germany will experience enormous growth until the year 2009. "The market size will increase from approximately 120 million € (2004) to 377 million €" (2009). "The federal government will be a major contributor to this development". In particular, the biometric procedures of fingerprint and facial recognition can profit from the government project. The ePass has been in circulation since November 2005, and contains a chip that holds a digital photograph and one fingerprint from each hand, usually of the index fingers, though others may be used if these fingers are missing or have extremely distorted prints. "A third biometric identifier – iris scans – could be added at a later stage". An increase in the prevalence of biometric technology in Germany is an effort to not only keep citizens safe within German borders but also to comply with the current US deadline for visa-waiver countries to introduce biometric passports. Germany is also one of the first countries to implement biometric technology at the Olympic Games to protect German athletes Ggorgi*[4]*. "The Olympic Games is always a diplomatically tense affair and previous events have been rocked by terrorist attacks—most notably when Germany last held the Games in Munich in 1972 and 11 Israeli athletes were killed".

Biometric technology was first used at the Olympic Summer Games in Athens, Greece in 2004. "On registering with the scheme, accredited visitors will receive an ID card containing their fingerprint biometrics data that will enable them to access the 'German House'. Accredited visitors will include athletes, coaching staff, team management and members of the media".

As a protest against the increasing use of biometric data, the influential hacker group Chaos Computer Club published a fingerprint of German Minister of the Interior Wolfgang Schedule in the March 2008 edition of its magazine *Datenschleuder .Wang [9].* The magazine also included the fingerprint on a film that readers could use to fool fingerprint readers.

INDIA

India is undertaking an ambitious mega project to provide a unique identification number to each of its 1.25 billion people Sathye *[5]*. The Identification number will be stored in central databases, consisting the biometric information of the individual. If implemented, this would be the biggest implementation of the Biometrics in the world. India's Home Minister, P Chidambaram, described the process as "the biggest exercise... since humankind came into existence". The government will then use the information to issue identity cards. Officials in India will spend one year classifying India's population according to demographics indicators. The physical count will begin on February 2011.

UNITED KINGDOM

Fingerprint scanners used in some schools to facilitate the subtraction of funds from an account financed by parents for the payment of school dinners. By using such a system nutritional reports can be produced for parents to surveil a child's intake Thornton *[6]*. This has raised questions from liberty groups as taking away the liberty of choice from the youth of society. Other concerns arise from the possibility of data leaking from the providers of school meals to interest groups that provide health services such as the NHS and insurance groups that may end up having a detrimental effect on the ability of individuals to enjoy equality of access to services.

5.0 RESEARCH PROBLEM

The intention is to understand and evaluate how biometrics might be used for mobile banking and payment systems, and to identify the best approach to take given the current state of the technology and the nature of most rural markets in the developing world. It assesses the potential of biometric security systems-user-based, not device-based-for mobile phones. As far as we know there is no other biometrically-enabled digital signature application available for mobile devices that can guarantee security by storing and processing all sensitive information on the device's SIM card. Biometric data never leaves the device's SIM card and can not be accessed except by the verification module which also runs on the SIM card; the user's biometric profile is completely safe. This is important to meet the highest privacy requirements.s we know there is no accessed, except by requirements

6.0 LIMITATION OF STUDY-

1. Research facility and money problem mostly common in research.
2. Purity of report depends on the respondents how willingly they have given the answer.
3. Also it is very important to study deeply about different states separately.
4. Research depends on the mutual relations but peoples don't understand the importance of study.
5. Importance of policies is very difficult to understand by common person.
6. Research depends on the correct response of customers and market both are variables in this research.

7.0 RESEARCH DESIGN AND RESEARCH METHODOLOGY

RESEARCH METHODOLOGY

Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research done scientifically. In study the various steps that are generally adopted by a researcher in studying his research problem along with logic behind them. Descriptive research studies are those studies which are concerned with describing the characteristics of a particular individual or of a group. So in that said research we use **descriptive and analytical method** to define importance and need of biometric system in mobile banking and security in organization. In this said research also describe the how much this are use in these sector and how much biometric system in the banking and organization. It's also important in said research to define how they create efficiency and smoothness in the work of organization and banking system. In this methodology we use secondary and primary data both to analyze the thinking and scope in the organization and banking areas. To find out the secondary data we use survey and observation method to identify the effect on consumer and other industries?

HYPOTHESIS

A hypothesis is a specific statement of prediction. It describes in concrete (rather than theoretical) terms what you expect will happen in your study. Not all studies have hypotheses. Sometimes a study is designed to be exploratory. There is no formal hypothesis, and perhaps the purpose of the study is to explore some area more thoroughly in order to develop some specific hypothesis or prediction that can be tested in future research. A single study may have one or many hypotheses.In said research we use null hypothesis in this thinking the security system always beneficial for organization and if it implement in the organization and banking areas it increase efficiency and control.

The **null hypothesis** typically corresponds to a general or default position. For example, the null hypothesis might be that there is no relationship between two measured phenomena, or that a potential treatment has no effect. In most legal systems, the presumption that a defendant is innocent ("until proven guilty") can be interpreted as saying that the null hypothesis is that the defendant is innocent.

RESEARCH DESIGN

This will discuss the various stages of the development of the proposed research model. First, the importance of context within the realm of biometrics is discussed as an introduction to the qualitative research that was conducted with Indian banks (SBI, ICICI, PNB, HDFC, AXIS BANK) to help determine what they felt might influence consumer perceptions about the acceptability of using biometric authentication. Next, further qualitative research was carried out to elicit any privacy and security concerns that may have been overlooked during the literature review. Finally, a proposed research model is presented and hypotheses developed.

7.1 PRELIMINARY QUALITATIVE RESEARCH – BANKS

In their attempt to thwart fraud, Indians banks are exploring a variety of avenues. Part of the impetus behind this initiative is the fact that Indians banks typically reimburse customers for any direct financial loses associated with fraud, again be it skimming a debit card or stealing a credit card, etc. To this end, four of the five major banks joined together to assist in reviewing the problem and investigate various ways of at least reducing the problem as they realize that it is unlikely that it will ever be completely eradicated.

In addition to the banks, the consortium consisted of representatives from various governmental and police organizations, as well as researchers from various Indian universities. Bank representation typically came from those areas responsible for privacy and/or security. Several meetings were held to assess the prevalence of identity fraud and discuss various alternatives to mitigate its occurrence. One of the areas of interest that came out of these discussions was the use of biometrics for customer identity authentication. Therefore, individual meetings, with personnel responsibility for privacy and/or security at the four banks, were suggested as a method to supplement the information gathered from the literature review.

Semi-structured exploratory interviews were conducted to establish which variables are most salient for consumer acceptance of biometric technology in the financial industry. When selecting interviewees, purposive sampling was used as outlined to insure reasonable representation from subject matter experts. This resulted in the identification of one individual from each of the four banks to be interviewed. As recommended by Miles and Huberman (1994), interviews continued as long as unique contributors were being identified. In this case conceptual saturation occurred quickly, after only 3 interviews. This was not surprising due to the high levels of industry communication, shared policies, and relative homogeneity within the Indian banking industry. All interviews were done in personally and via Phone. The phone interview lasted approximately 45 minutes while the in-person interviews went longer and took approximately 75 minutes.

Cognitive interviewing techniques were used to minimize interviewer bias as recommended by Willis (1999). This included the "think aloud" technique outlined in Willis (1999), which encourages respondents to verbalize their thought processes as they respond to the questions. This technique allows a more sophisticated understanding of complex issues to emerge as the interviewer is exposed to the interviewee's reasoning, not simply their responses. The interviewer also paraphrased the responses throughout the interviews to ensure correct interpretations of respondent's statements were made.

Initial Banks interview questions included the following:

1. Does your bank have a vision and/or plan regarding biometrics?
2. Do you believe that vision is shared by other banks and financial institutions?
3. Do you think customers are satisfied with the existing level of security offered by financial institutions?
4. What would your bank like to know with respect to people's perceptions of biometrics?
5. Do you see any issues that might impede biometric adoption within the Indian banking industry?
6. In what contexts, scenarios, or applications would you like to examine consumer acceptability of biometric authentication technology?

Initial customer interviews questions include the following:

1. What you think how much biometric system safe for mobile baking and other facilities?
2. In what context you feel that mobile banking profitable and safely way for doing Purchasing or transaction?
3. Are you feeling that's more comfortable than other banking facilities?
4. How much you know about Biometric system and how you hope Indians accept this change in banking sector?
5. Are you fulfilling basic requirement which needed for Biometric access? (That's instrument base question)

Data analysis was conducted after each interview, allowing questions to change over time in response to emerging categories. Data categorization and descriptive and pattern-based coding were used.

The results of the interviews with the bank employees are laid out as follows.

Table 3-1 lists the results of the initial discussion with the three bank representatives in order of the points raised. Table 3-2 lists possible contexts that the bank employees felt it would be worthwhile examining as context was envisioned as being an influencing factor in consumer perceptions about biometric identity authentication technology. For those contexts that they felt were worthy of exploring, they were also asked to rank them in order of importance; this ranking is provided in the table.

TABLE 3-1: KEY INSIGHTS PROVIDED BY BANK PERSONNEL

Bank#I (ICICI)	
1	Unlikely to be pursued unilaterally by their bank, or any other Indian bank.
2	Banks need to collectively assess the tradeoffs between consumer perceptions, cost, and the level of security biometrics provide their customers.
3	In terms of customer perceptions, where do their responsibility for security end and the banks' begin?
4	What do customers see as the key benefits and drawbacks of using biometrics?
5	Do people understand biometrics?
6	Finger recognition biometrics is already being used for telephone banking, but this is not considered a "high" security application.
Bank #2 (SBI)	
1	Unlikely to be pursued unilaterally by their bank, or any other Indian bank.
2	In terms of customer perceptions, where do their responsibility for security end and the banks' begin?
3	Do people understand biometrics?
4	What do customers see as the key benefits and drawbacks of using biometrics?
Bank #3 (HDFC)	
1	Wonders if biometrics is a solution in search of a problem.
2	Unlikely to be pursued unilaterally by their bank, or any other Indian bank.
3	In terms of customer perceptions, where do their responsibility for security end and the banks' begin?
4	Interoperability concerns.
5	Do people understand biometrics?
6	What do customers see as the key benefits and drawbacks of using biometrics?
7	Will the introduction of chip technology on credit cards confuse consumers and, as such, confound the results of the survey?

Table 3-1 shows considerable consistency in terms of how Indian banks view biometrics in general. Given the nature of the Indian banking industry, it was unanimous that biometrics was viewed as something that would be pursued by all the banks or none of the banks. This was due to two considerations.

First, there are five major Indian banks that collectively have a significant share of the consumer banking market but that individually do not have enough clout to be market leaders. Therefore, if any one of them unilaterally decided to pursue customer identity authentication via biometrics and it was not well received, it could cost them market share and the associated profits; and this would be in addition to the substantial upfront costs of installing the technology. Even if it was embraced by customers such that it created initial competitive advantage, this would not be sustainable simply because the technology is widely available and, hence, could be easily replicated relatively quickly by the other four banks. However, if the five Indian banks deemed that it was in their best interests, most likely from a cost-benefit perspective, to introduce biometrics and collectively agreed to do so at approximately the same time, this would mitigate the possibility of any major redistribution of market share should there be consumer backlash simply because of the limited options available to the Indian consumer.

The other consideration as to why Indian banks would pursue it collectively is due to the existing technological infrastructure with respect to debit cards. While the initial rollout of identity authentication using biometrics would be at bank ATMs, the feeling is that it would inevitably become more widespread such that it would be used essentially wherever you use a debit card. Given this envisioned pervasiveness, banks would have to involve those companies (e.g. Interac) that control the debit card industry and the associated protocols. Again, from both a cost-benefit and competitive standpoint, this is yet another impediment making it unlikely that any Indian bank would initiate biometric identity authentication individually [11].

Examining other general discussion points, all three interviewees wondered what people thought with respect to where a customer's responsibility for security ended and the bank's responsibility began. As the focus of this research was acceptability of biometrics for identity authentication, this issue was not addressed given the difficulty of operational sing this concept.

The other common concern was whether or not people would understand what was meant by the term "biometrics". In order to address this concern, there would be appropriate wording in the questionnaire defining the term.

Looking at the potential contexts in Table 3-2, there was a good degree of consistency in terms of what were perceived to be the most relevant contexts to examine, and unanimous agreement on the ranking of the top two contexts: voluntariness and control. The importance of whether using biometrics should be voluntary or not is relatively self-explanatory. As mentioned previously, all bank personnel were of the opinion that either the five biggest Indian banks would adopt biometric identity authentication, or none of them would. Given this statement, combined with their collective market share and a lack of viable options for the Indian consumer, one might wonder why they would consider voluntariness an issue. The answer is basic customer service. If consumers don't want, or worse are opposed to, biometric identity authentication, than why pursue it, especially given the implementation costs involved.

Granted, with only five major banks, the Indian banking industry gives consumers limited options presently, but that doesn't mean other institutions (i.e. credit unions and smaller banks) won't try to take advantage of any significant customer backlash. Whether or not customers would pursue alternatives (i.e. smaller

banks or credit unions) simply due to being forced to use biometrics is debatable, but these smaller market players would inevitably try to leverage any customer discontent to their advantage.

TABLE 3-2: RANKING OF POSSIBLE CONTEXTS TO CONSIDER IN EXAMINING CONSUMER PERCEPTIONS OF BIOMETRIC AUTHENTICATION TECHNOLOGY AS IDENTIFIED BY BANK PERSONNEL

Possible Context	Ranking		
	Bank#l	Bank #2	Bank #3
Voluntary versus involuntary	1	1	1
Bank control versus shared control	2	2	2
Type of application (debit card, credit card, etc.)	3		
Online use versus ATM use versus POS use			3
Type of biometric	4	3	
Safety deposit boxes	5		4
Applicable only to new customers	6	2	5

In terms of control, this was framed in terms of where the biometric information is stored. Bank control means it is centrally stored by the bank. Shared control means that only a portion of the information is centrally stored by the bank, and the remainder is stored on a "smart card" retained by the customer. In the latter case, the information stored at the bank is useless without being combined with the information from the card, and vice versa. What this means in terms of a consumer's privacy calculus is that while the benefit of convenience is lessened (i.e. the consumer still doesn't need a password, but they now require the card), the "cost" of privacy and security also drops (i.e. the information stored by the bank is incomplete and, therefore, useless regardless of whether it is shared or stolen). While the bank personnel viewed this as key given people's reticence towards the amount of information being captured in general, and by banks in particular, it also aligns well with the conception that the issue of control is central to consumers' privacy perceptions as previously discussed.

Beyond these two issues, type of biometric and application (i.e. debit cards versus credit cards) were deemed areas worthy of investigation by two respondents, while one interviewee suggested that it would be interesting to examine whether there would be any difference based upon ATM use versus online use versus POS (point-of-sale) use. Interestingly enough, no one saw the importance of testing the acceptance of multi-modal (i.e. two or more biometrics, biometric and a password, etc.) authentication methods as they did not foresee that as being offered by the banks.

Two of the interviewees thought examining the acceptability of biometrics within the context of safety deposit boxes would be worthwhile as they envisioned the initial use, or testing, of biometrics potentially being to access safety deposit boxes: This was based upon the premise that, on average, people tend to keep highly valuable assets (be they financial or nonfinancial) in safety deposit boxes, combined with the fact that they are typically used infrequently. The latter point often leads to lost keys and/or forgotten passwords; standalone biometrics (i.e. no shared control with a smart card) would address these problems quite well. Despite the above positive aspects of looking at this application, it was dropped due to the fact that considerably more people tend to have debit cards and use ATMs versus having safety deposit boxes. Ultimately, the aspects of voluntariness and control were the top two choices among the three interviewees and, as such, were the ones chosen for investigation.

Looking at demographics, all three bank employees identified age, gender, income level, and education as being worthwhile to examine. The former two align with previous research as age and gender have been shown to impact technology adoption. Income level was considered salient as it is presumed that people with higher income would typically have more financial assets available via debit cards. As such, they may be more amenable to the use of what is a more secure method of identity authentication, presuming, again, that their perceived benefits outweigh their perceived concerns/costs. Similarly, people that are more educated may have a better understanding of what biometrics can and can't do which may influence their perceptions.

7.2 PRELIMINARY QUALITATIVE RESEARCH - UNDERSTANDING PERCEIVED BENEFITS AND CONCERNS

The privacy and security concerns and usefulness were discussed as factors that influence the attitudes and/or adoption intentions of consumers with respect to certain types of technology such as the internet, m-commerce, and u-commerce.

Furthermore, the discussions with bank personnel indicated that they would like to know what consumers see as the key benefits and drawbacks of using biometrics. Therefore, given the lack of research with respect to factors influencing biometric adoption, it was deemed necessary to obtain a better understanding of the key perceived benefits and concerns that are top-of-mind for consumers prior to the development of the proposed research model and related hypotheses.

7.3 RESEARCH METHODOLOGY

Data was gathered via an online survey. A description of fingerprint biometric authentication for ATM transactions was provided and subjects were asked the following three open-ended questions:

1. What do you feel are the benefits/advantages of using biometrics?
2. What concerns do you have using biometrics?
3. Please provide any other comments regarding the use of biometrics.

A total of 367 usable surveys were obtained from across Delhi Region. There was a roughly equal representation from the demographic perspectives of gender and age, the latter ranging from 18 through to over 55. In terms of education, the majority of respondents had at least some college or university education. Looking at income level, approximately half of the respondents made Rs. 50,000 or less, while roughly 10% preferred not to answer. All subjects were above 18, used an ATM and mobile banking, and were not employed by financial institutions.

The data was analyzed using a three stage iterative process. In the first stage, respondents' answers to the questions were reviewed and open coding was used to identify shared characteristics and generate initial descriptive categories. The second stage consisted of scrutinizing the initially identified categories and integrating them into more centralized categories. In the final stage, the use of pattern coding allowed the clustering of these centralized categories into overriding themes. While the first and second stages were conducted by one researcher, the final stage was done through meetings and discussion with two other researchers during which the responses were reviewed for consistency and to build consensus.

Answers to the three open-ended questions were copied into a qualitative analysis program called NVivo. After the first and second stage analyses, the following general Categories were identified as concerns of using biometric verification in the context of Mobile transactions:

1. How secure is my information from hackers/insiders?
2. My fingerprints can be copied.
3. The increased possibility of identity theft.
4. Inconvenience.
5. Inability to share banking responsibilities with others.
6. Reliability of the technology in terms of startup glitches, ongoing maintenance issues, and accuracy of the fingerprint reader due to dirt, grease, etc.
7. Slower access to accounts.
8. What happens if my fingers are damaged, or if they become damaged?
9. What happens when I go overseas and they aren't using biometrics at ATMs?
10. Its too much information for the banks to have.
11.1 don't like supplying biometric information to the bank.
12.1 am concerned about my privacy.
13. How well will my privacy be protected?

14. Will my biometric information be used for reasons beyond those intended (i.e. shared with other corporations, law enforcement, governmental agencies, etc.)?
15. Physical harm as thieves will now severe my fingers and/or hand to gain access to my account.

The third stage analysis resulted in the synthesis of the twelve concern categories into five recurring themes. They were:
1. Security Concerns (Items 1 through 3)
2. Inconvenience (Items 4 through 9)
3. Privacy Issues (Items 10 through 13)
4. Function Creep (Item 14)
5. Physical Harm (Item 15)

The NVivo analysis revealed the following 13 general benefit categories in the first and second stage analyses:
1. Increased security
2. Increased safety
3. Difficulty in reproduction of fingerprints
4. Deterrent to identity theft
5. I am the only one with access to my accounts
6. Less chance of theft from my accounts
7. Less chance of theft of my PIN/password
8. Less concern if I lose my card
9. Easier to use
10. No chance of forgetting your card
11. No PIN/password to remember
12. Convenience
13. Faster access to accounts

The third stage analysis, again, conducted in conjunction with two other researchers through meetings and discussions, resulted in the synthesis of the thirteen broad benefit categories into two overriding themes due to the sufficient commonality identified among the second stage categories. The two higher level benefit constructs identified were:
1. Increased Security (Items 1 through 8)
2. Convenience (Items 9 through 13)

8.0 RESULTS AND DISCUSSION

Looking at Table 3-3, the concerns, ranked by order of number of mentions, are security, inconvenience, function creep, privacy, and physical harm. Security was the greatest concern for people and by a considerable margin as it was cited as an issue by 145 respondents, which represents almost 40% of the usable surveys. Typically, respondents were worried about the ability of thieves to access their biometric data thereby giving them access to their financial information and assets as is exemplified by the following comments: *"Anyone could hack into the system and take information'"; "If identity theft occurred, it would be far worse than now.'"; "I have concerns about fingerprints which I think can be copied."; "Somebody somehow getting my fingerprint to access my account"; "Fingerprints left on ATMs may be lifted and used by those who know how"; "Overall security is a concern because there are ways to replicate fingerprints.*"

TABLE 3-3: CONCERNS OF USING BIOMETRIC AUTHENTICATION AT ATMs

Concern	Number of Mentions	Percent of Respondents
Security	145	39.50%
Inconvenience	99	27.00%
Function Creep	81	22.10%
Privacy	77	21.00%
Physical Harm	38	10.40%

Of particular interest was the finding that some people believe that it is the actual biometric that is stored when, in actuality, recall that the biometric is converted into a mathematical expression which is then stored as the template for identity authentication.

Currently, it is not possible to reverse engineer a viable biometric from the encrypted mathematical expression. Inconvenience was the second most cited concern as it was mentioned by 99 people, or 27% of the survey participants. The biggest issue around inconvenience seemed to be the inabilities to have someone else do your banking for you. Despite bank direction to the contrary, it would appear that some people are in the habit of sharing banking duties with their friends and significant others. Unfortunately, the implementation of biometric authentication would make it impossible for this practice to continue. Presumably, shared accounts will be able to be accessed by either owner providing their fingerprint for authentication, but for those relationships where the parties prefer to have separate bank accounts; this may be a significant hurdle with respect to acceptance. Beyond this aspect, the issues of being incapacitated, startup glitches, and ongoing reliability were also mentioned. Some of the responses within the inconvenience context included:

"Sometimes I give my bank card to my significant other or close friends or relatives to withdraw money or deposit cheques for my business. They would not be able to do this"; "Personally, I allow my fiancée to access my bank account. Whoever has the free time that day takes both cards and pay cheques or withdrawals and runs to the bank for us both.'"'; "If I am sick and unable to go to the bank to get money, my partner would not be able to go for me. "; "The time it will take to get the system running without any glitches (but it's standard with any new thing) "; "The technology is still young and imperfect"; "Early models flawed. Quality of biometric reading component, not working"; "Could be more complicated, and I have my doubts concerning the reliability of the new system ".

Function creep was mentioned by 81 respondents, which represents just over 22% of the usable surveys. Recall from Section 2.2.1 that function creep refers to the concern that the initial use of biometric-based systems will morph and expand, innocently and/or covertly, into other areas not previously envisioned or agreed to by those enrolled in this type of authentication mechanism. Also as previously stated, CRISIL (2008) suggest that function creep may be one of the biggest impediments to widespread biometric use due to current information sharing practices amongst for-profit and governmental organizations. In fact, some law enforcement information systems have been sold based upon their ability to assimilate information from an array of various databases. Some of the responses were:

"I would not accept this service unless there was legislation in place where NO one else could access this information, including the government"; "Banks releasing my fingerprint to other companies/agencies.'"; "I am concerned that the info could be made available to the government or any other agency as well"; "Who else will be able to get their hands on this biometrics and use if for other situations?".

Privacy was close behind function creep as 77 people, or 21% of the survey participants, mentioned it as an issue. Responses included:

"Privacy is important to all of us and by using this we are giving out way too much"; "I don't like the idea of someone having that much information about me"; "I don't know that I like the idea of providing my bank with my fingerprint, although not for any definable reason, I just feel that it's very personal"; "Biometrics is more secure but we have to make sure that our privacy and our rights remain protected at all cost."; "*I am concerned about misuse of the technology and the potential of loss of privacy.*"

Finally, while the concern that garnered the least number of mentions was the threat of physical harm, it was still mentioned by 38 people, or just over 10% of those surveyed. While there are viability tests to help ensure that the biometric being authenticated is coming from living tissue, this may be of little comfort in

the minds of consumers given that the present system just requires one to surrender their debit card and PIN to a would-be thief thus potentially avoiding physical violence more so than when one is dealing with a piece of oneself. Comments with regard to this concern included:'

Fear the crime that might take place against the person. Now if a thief wants access to your account, they simply steal your card even if that means knocking you out for it. In this new scenario, the thief would have to basically kill you to steal your finger.";"I would also be concerned about people attacking me, cutting off my finger, and using it to access my account. Then I've lost money and a finger."; "People cutting off fingers to rob someone.''; "Please be aware that criminals will use whatever means they have to in order to steal, and therefore they may cut off fingers to gain access etc.";"Someone cutting your finger off to access your account"; "The Hollywood scenario to cut the finger off to access bank accounts is more probable."

In addition to the above findings, another trend was noted that lends support to the Notion espoused by Narshima committee (2008) that perhaps there is not a clear distinction between privacy and security in the minds of consumers, at least within the context of biometric authentication technology for accessing one's bank accounts. When people discuss privacy and security concerns from this perspective, many of them tend to mention more than one dimension of either privacy, security, or both. Of the 367 respondents, 92, or just over 25%, mentioned both privacy and a security concern. When multiple mentions of privacy concerns or security concerns are added to this group, the number jumps to 142 participants, or almost 39%. Some of the comments that exemplify this phenomenon are as follows:

"Privacy is important to all of us and by using this we are giving out way too much. In the past people have hacked cards, etc. and if they ever hacked into this it would be a nightmare. "; "I would be concerned about the bank having personal material on me, such as my fingerprint, and how this could be used by hackers and police. "; "Too much info and not enough safeguards. "; "My personal information could be sold, offered, stolen, etc. by, or to, other parties. "

Moving on to benefits, the findings are summarized in Table 3-4. Increased security was mentioned as a benefit by 203 respondents which equates to just over 55% of the total, while convenience was cited by 97 people or just over 26% of the survey participants. Some of the comments made regarding security were: "*/ think in itself it should be more secure because no one has the same fingerprints"; "Less chance of someone else stealing my identity.*"; "*/ wouldn't need to worry about someone stealing my PIN number (whether by watching over my shoulder or on security cameras, etc). I'd feel more secure that my money couldn't be accessed as easily"; "I feel that it will increase the security regarding personal banking"; "You feel more secure in knowing that only you can access your bank account, because nobody else has the same fingerprint as you"; "Foolproof identification and protection of my banking transactions"; "It would be another layer of security to protect my identity"; "I think maybe it would be more secure than a bank card because only one person has your fingerprint... YOU!"*

TABLE 3-4: BENEFITS OF USING BIOMETRIC AUTHENTICATION AT ATMS AND MOBILE BANKING

Benefit	Number of Mentions	Percent of Respondents
Increased Security	203	55.30%
Convenience	97	26.40%

On first glance, it seems odd that security is identified as a benefit by over 55% of the respondents while being simultaneously cited as the primary concern by almost 40% of the survey participants. However, upon further review of the answers, the respondents appear to be discussing two different points of view. When security is mentioned as a benefit, it is typically within the context of access to financial data (i.e. only I can access my accounts, the bank is sure it is me, etc.). When security is mentioned as a concern, it I s typically mentioned within the context of the bank not having appropriate safeguards to protect the biometric data itself. In several cases, respondents mention both contexts in the same sentence saying that it will be a much more secure method of verification for access to financial assets provided the security around the biometric data is sufficient.

This is exemplified by the following sample of comments: *"If it could be guaranteed (the security) I would like it very much, because I think in itself it should be more secure because no one has the same fingerprints"; "As long as the other [biometric] information is kept safely at the bank, I believe this is a great security upgrade and will prevent identity theft"; "I know the day is coming, and this would seem to be more secure than a card access with a PIN number. As long as the security of the biometric information can be guaranteed (as much as any security can be), then this would be a great move"*

A similar phenomenon can be seen in terms inconvenience versus convenience in that 99 respondents, or 27%, mentioned the former as a concern while almost the same number (97 respondents, or just over 26%) mentioned the latter as a benefit. However, unlike security in which it appears that the respondents seem to be discussing two different points of view, in looking at inconvenience and convenience, it seems to be more of a paradox in that participants are looking at opposite sides of the same issue. In other words, if they adopt biometric authentication they will have the convenience of no longer having to use debit cards and PINs, but will have to give up the convenience of being able to get someone to do their banking for them.

Upon further analysis of the micro-level classifications, the convenience benefits are typically: (i) not having to remember a card and/or PIN; (ii) faster service; and (iii) it being easier to use. Remarks made with regard to convenience include: '*you need to have a debit card or [to] remember a password"; "It would be a faster way to access my money"; "You can't forget your fingerprint"; "No pin numbers to remember"; "Fast, convenient, don't have to search for debit card or risk forgetting the PIN"; "No more carrying a card around, don't have to know a PIN, don't have to worry about losing your card"; "It's one less password to forget."*

9 CONCLUSION AND FUTURE DIRECTIONS

The empirical results represent an important first step in understanding consumers' attitudes towards using biometrics as a means of identity authentication at ATMs. However, as with most research, the findings suggest a variety of additional directions that should be considered.

While consumers appear to understand the value of using biometrics for identity authentication at their banks, what should be explored is whether or not the positive effect of usefulness upon attitude outweighs the negative effect of privacy and security concerns. It would be interesting to determine at what point these two conflicting concepts balance out in the minds of consumers, a "tipping point" if you will, such that the consumer is ambivalent towards the use of biometrics. As it is unlikely that this balance would remain static across applications, the impact of various scenarios and contexts should be examined. However, this would merely be a starting point. Examining the responses to the open-ended questions, it would appear that the consumer is simultaneously evaluating a myriad array of conflicting factors when determining the value of biometric authentication. Looking at control for example, as consumer control increases, so does their attitude towards using biometrics. In addition, their privacy and security concerns drop; but so does usefulness. In other words, increased control would appear to make consumers feel better about the prospect of biometrics, presumably due in part to the reduced privacy and security concerns; but this is being mitigated by the loss of convenience associated with now being required to carry a card as with the present debit card system, albeit the latter requires a PIN, which can be forgotten. Furthermore, based upon the initial qualitative study and subsequently demonstrated in the answers to the open ended questions in the final survey, consumers simultaneously see security as a concern and an advantage; and, in conditions of shared control, this advantage is seen as greater, and the concern less, than in the context of bank control. The nature of some of the comments made in the open-ended questions suggests that Indians may not have the background or knowledge with respect to how biometrics work and why they can be much more secure than other classical forms of security. As mentioned previously, this underscores the need for public education; but the question remains as to what should be taught and what would be the impact. Presuming that the banks wish to pursue using biometrics for identity authentication, it would be useful to measure people's initial understanding of biometrics generally and under the proposed context, provide some education through various forums and media, and then measure people's subsequent understanding. This would allow the banks to assess the impact of various educational alternatives which should consequently lead to a better allocation of scarce marketing resources and, hopefully, to a more positive attitude with respect to the use of biometrics in the Canadian banking industry. Institutional trust was found to influence attitude both directly and indirectly. While the direct impact of institutional trust on attitude was significant ($p < 0.05$), it appears to have a more indirect influence through privacy and security concerns. This mediation effect should be examined further in future research, under varying scenarios and contexts. This research reaffirmed the importance of control in the minds of consumers when considering initiatives that are perceived as having privacy implications. Recall that it was demonstrated that control was significant when enrolment in the biometric identity authentication program was mandatory, but was not significant when the program was voluntary. It was suggested that this may be due to the supposition by consumers that a voluntary program gives the consumer de facto control in the sense that they don't have to enroll in the first place. Further investigation is needed to fully understand this phenomenon as

examining the interaction of control and voluntariness could provide for some interesting future research that could offer practitioners valuable insights as to what the most effective strategies might be when deploying biometric identity authentication technologies. The previous paragraphs suggest future research along the lines of how to expand upon the concepts and constructs in the proposed model. However, a variety of other avenues for continuing research exist beyond the model. First, as alluded to in the limitations section, only fingerprints were examined in this research. While this biometric does enjoy a significant market share, face recognition and iris recognition are also quite popular. Also, as face recognition becomes more accurate it will probably attract more of the market. Looking at iris recognition, this is considered to be the most reliable biometric available. However, the costs of the scanners make it prohibitively expensive for widespread use at the present time; but as the costs come down, it may replace fingerprints as the market leader. Then there are the emerging biometrics. This suggests that similar research is required to assess consumer perceptions of acceptability of alternative biometrics. This research examined consumer acceptability within the financial sector. Given the interests of governments with respect to biometrically enabled documents and of businesses regarding more accurate time and attendance, to name just two potential markets, further research could examine acceptability across a variety of potential applications. Recall from the qualitative research done with bank personnel that a number of different contexts were identified as being worthwhile to investigate, and this was strictly within the realm of the Canadian banking industry. There are probably a considerable number of contexts of interest to a variety of organizations. These contexts could be examined individually, or in conjunction with other circumstances, to assess how they interact with one another.

10. REFERENCES

1. Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn, P; Ross, A. *Handbook of Biometrics*. Springer.
2. EITO; "European Information Technology Observatory 2004", Edition 15, Brussels, 2004.
3. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, pp. 614-634, 2001.
4. Georgi, F. and J.Pinkl; "Mobile Banking in Deutschland- Der zweite Anlauf', in Die Bank, Berlin, Issue 3/2005, p. 57-61.
5. Sathye, M. "Adoption of internet banking by Australian consumers: an empirical investigation," *International Journal of Bank Marketing*, Vol. 17 No. 7, pp. 324-334, 1999.
6. Thornton, J. and L. White, "Customer orientations and usage of financial distribution channels," *Journal of Services Marketing*, Vol. 15 No. 3, pp. 168-185, 2001.
7. Friedman, B., P.H. Kahn Jr. and D.C. Howe, "Trust online," *Communications of the ACM*, Vol. 43, No. 12, pp. 34–40, 2000.
8. Gefen, D., E. Karahanna, and D.W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly,* Vol. 27, No. 1, pp.51–90, 2003.
9. Wang, Y.S., Y.M. Wang, H.H. Lin, and T.I. Tang, "Determinants of user acceptance of internet banking: An empirical study," *International Journal of Service Industry Management*, Vol. 14, No. 5, pp. 501–519,2003.
10. Luarn, P. and H-H. Lin, "Toward an understanding of the behavioural intention to use mobile banking," *Computers in Human Behaviour*, Vol. 21, No. 6, pp. 873-891, 2005.
11. S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric Hash Functions for Fingerprint Minutiae," Proc. Int'l Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance, pp. 30-38, 2005

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals