Summer 2005

Electronic capture and analysis of fraudulent behavioral patterns : an application to identity fraud

Benjamin Ngugi
New Jersey Institute of Technology

ABSTRACT

ELECTRONIC CAPTURE AND ANALYSIS OF FRAUDULENT BEHAVIORAL PATTERNS: AN APPLICATION TO IDENTITY FRAUD

by
Benjamin Ngugi

The objective of this research was to find a transparent and secure solution for mitigating identity fraud and to find the critical factors that determine the solution's acceptance.

Identity fraud is identified as a key problem with total losses exceeding fifty two billion dollars (Javelin Strategy and Research 2005). A common denominator in most identity-fraud-prone transactions is the use of a keypad; hence this research focuses on keypad data entry and proposes a biometric solution. Three studies develop, evaluate and investigate the feasibility of this solution.

The first study was done in three stages. Stage one investigated the technical feasibility of the biometric keypad, stage two evaluated the keypad under different field conditions and stage three investigated acceptable user parameters. A key shortcoming with current authentication methods is the use of external identifiers that are prone to theft, unlike biometric patterns. A biometric keypad that supplements the present external identifiers was proposed, prototyped and evaluated. The results demonstrated that a biometric keypad can be a feasible medium performance solution. Addition of pressure and higher typing speeds were found to enhance discrimination accuracy while typing patterns were found to vary with elapsed time which led to deterioration in accuracy.

The second study interviewed executives with experience in the introduction of new technologies with the objective of identifying and ranking critical factors that are important in the adoption of new biometrics. Performance, ease-of-use and trust-privacy issues were the most cited factors. A biometric acceptance model was formulated and five hypotheses were proposed from these interviews and prior research. Executives rated the keypad's ease-of-use high in comparison to other biometric approaches but were concerned about its accuracy.

The third study was a user attitude survey whose objective was to validate the formulated biometric acceptance model and acquire data on acceptable usage parameters. The proposed biometric model was validated and the proposed hypotheses were supported. Acceptable error rates and training times indicated that the biometric keypad would be more complex to engineer.

The dissertation concludes by summarizing the contributions and limitations of the three studies followed by several suggestions for future research.

ELECTRONIC CAPTURE AND ANALYSIS OF FRAUDULENT BEHAVIORAL PATTERNS: AN APPLICATION TO IDENTITY FRAUD

by
Benjamin Ngugi

A Dissertation
Submitted to the Faculty of
New Jersey Institute of Technology
In Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy in Information Systems

Department of Information Systems

August 2005

APPROVAL PAGE

ELECTRONIC CAPTURE AND ANALYSIS OF FRAUDULENT BEHAVIORAL PATTERNS: AN APPLICATION TO IDENTITY FRAUD

Benjamin Ngugi

7/15/05

Dr. Michael Recce, Dissertation Co-Advisor — Date
Associate Professor of Information Systems, NJIT

8/10/05

Dr. Marilyn Tremaine, Dissertation Co-Advisor — Date
Professor of Information Systems, NJIT

7/15/05

Dr. George Widmeyer, Committee Member — Date
Associate Professor of Information Systems, NJIT

7/15/05

Dr. David Mendonca, Committee Member — Date
Assistant Professor of Information Systems, NJIT

7/15/05

Dr. Joseph Wilder, Committee Member — Date
Research Professor, Center for Advanced Information Processing (CAIP), Member, Graduate Faculty, Electrical and Computer Engineering, Rutgers University.

BIOGRAPHICAL SKETCH

Author: Benjamin Ngugi

Degree: Doctor of Philosophy

Date: August 2005

Undergraduate and Graduate Education:

- Doctor of Philosophy in Information Systems

  New Jersey Institute of Technology, Newark, New Jersey, USA, 2005

- Master of Science in Information Systems (transferred)

  University of Nairobi, Kenya, 2001

- Bachelor of Science in Electrical Engineering

  University of Nairobi, Kenya, 1990

Major: Information Systems

Publications and Presentations

Benton, M., Kim, E., and Ngugi, B. "Bridging the Gap: From Traditional Information Retrieval to the Semantic Web," Proceedings of the Eighth American Conference on Information Systems, Dallas, TX, 2002, pp. 1448-1455.

Ngugi, B., Tremaine, M., and Recce, M. "Fighting Identity Fraud with the Addition of Biometric Techniques," Proceedings of the Tenth Americas Conference on Information Systems, New York, NY, 2004, pp. 4419-4422.

Ngugi, B., Tremaine, M., and Recce, M. "Secure and Transparent User Authentication at the Human-Computer Interface," New Jersey Homeland Security Conference, Fort Monmouth, NJ, 2004.

This dissertation is dedicated to my late mother, Phyllis Wabari, for showing me the importance of honesty and hard work; to my father, Francis Ngugi, for daring to dream big; to my wife, Mary Kinyanjui, for enduring love; and to my children; Bernice, Maureen and Edna, for giving me another reason to work harder.

ACKNOWLEDGEMENT

My deepest gratitude goes to my co-advisors Drs. Michael Recce and Marilyn Tremaine for guiding and supporting me throughout the dissertation process, to my committee members, Drs. David Mendonça, George Widmeyer and Joseph Wilder for their dedication and feedback on the dissertation deliverables, and to Dr. Roxanne Hiltz for support given throughout my doctoral program.

I also wish to thank all the other faculty members, Ph.D. students and departmental staff for their support. Special thanks go to Eunhee Kim, Peishih Chang, Dezhi Wu, Suling Zhang, Edward Mahinda, Morgan Benton, Razvan Bot, Xin Chen, John Lacontora and Mojgan Mohtashami for helping in various ways. Lastly, I want to thank all those who participated in my experiments, interviews and surveys. Without their contribution, this dissertation would not be.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

Chapter **Page**

TABLE OF CONTENTS
(Continued)

LIST OF TABLES

LIST OF TABLES
(Continued)

LIST OF TABLES
(Continued)

LIST OF FIGURES

LIST OF FIGURES
(Continued)

CHAPTER 1

INTRODUCTION TO RESEARCH PROBLEM

1.1 Introduction

The key motivation for this work is the enormous problem that modern society is having with identity-fraud. This dissertation addresses one area of this problem, that is, the problem of authenticating that someone, who is typing in a password or personal identification number (PIN) for access to private information or resources, is the true owner of that information or resource. The dissertation proposes a solution to the authentication problem which is the capture of the unique signature that each individual has when they type in a PIN or password and use this unique signature to authenticate this person at a later time. This authentication method is called a keypad biometric. The dissertation develops this method through pattern recognition techniques and then evaluates it through a series of user studies that represent the real life parameters that such a method would need to work under. It then turns its attention to issues with the acceptance of such a method, first by studying executives who are likely to make the decisions on whether to implement a keypad biometric and then by studying end users perceived responses to the introduction of a keypad biometric.

This chapter traces the growth of the information driven economy and relates this growth to the growth of identity fraud. It notes that the growth of personal computers and the Internet have revolutionized the way people conduct business and that the flip side of this growth is a proliferation of personal information databases. This proliferation and the increasing remoteness of the access has led to an increased uncertainty in the authenticity of the accessing party.

This has led to a set of unscrupulous people who have taken advantage of this uncertainty leading to a large increase in identify fraud. Data is cited that indicates that identity fraud is a key national problem that needs to be addressed. Thus, this research on biometric authentication can be one contribution to solving this problem. Finally, at the end of this Chapter, the structure of the rest of the dissertation is given.

1.2 Growth of Identity Theft

The last two decades have witnessed an unprecedented growth of computers. As predicted by Moore's law (Moore 1965), computer speeds have approximately doubled every eighteen months, CPU prices continue to drop, and network speeds are similarly increasing. The Internet has grown to unprecedented levels. In the United States *54 million households, which is 51 % of the total U.S. population had one or more computers. 44 million households which is 42 % of the U.S. population had at least one member who used the Internet* (U.S. Census Bureau 2001). Electronic commerce has spread its tentacles to cover most goods sold in the nation. The average person can now conduct most basic life management services like paying bills, buying products, stocks and insurance on the Internet.

The flip side of all this progress is a proliferation of personal identity information over disparate databases and an increase in uncertainty of the authenticity of the remote party, accessing the information and resources. These two issues have increased the levels of identity fraud to unprecedented levels.

1.2.1 Definition of Identity Theft

The term identity theft comes from a combination of two words ***identity*** and ***theft***

Identity can be defined as the *distinguishing character or personality of an individual* (Merriam-Webster 2003) while ***theft*** is defined as the *act of stealing; specifically: the felonious taking and removing of personal property with intent to deprive the rightful owner of it* (Merriam-Webster 2003). ***Identity theft*** involves *stealing of another person's personal identifying information such as social security number, date of birth and mother's maiden name, and then using the information to fraudulently establish credit, run up debt or take over existing financial accounts (U.S. General Accounting Office 2002).*

The term ***identity theft*** should strictly refer to the stealing and unauthorized use of the stolen documents while the term *identity fraud* should refer to the resulting crimes that are committed using the stolen or fraudulent identifiers and documents (Gordon and Willox 2003). The two phrases are used interchangeably in this dissertation because much of the literature in this area does not make this distinction and because the focus of this dissertation is on authentication which can be a method for preventing identity theft and identity fraud.

1.2.2 The Extent of Identity Fraud

Identity theft has been the leading fraud in the United States for the last four years in a row (Javelin Strategy and Research 2005). About nine-million Americans became victims of identity theft in 2004 with an average loss of $5,686 per victim, which gives an annual identity fraud cost of $52.6 Billion (Javelin Strategy and Research 2005). Victims

are usually insured from direct losses incurred on their accounts, but they still ended up paying more than $5 billions in out-of-pockets costs. This type of loss continues to increase. The time wasted by the victims to resolve the problems created by the misuse of their personal information and to restore their credit-worthiness is approximated to be 300 million hours.

The cost to the business community is even higher. It is approximated that the losses suffered by the business communities are about $279 billion dollars without considering recovery expenditures (Identity Theft Resource Center Inc. 2003). The identity theft problem is global and threatens many nations. In the United Kingdom, identity theft was estimated to cost more than 1.4 billion British pounds as early as the year 2000 and with an increase of 54% per annum (Economics and Domestic Secretariat 2002).

1.2.3 Role of Identity Theft as a Breeder Crime

The above facts show that the losses resulting from identity theft are enormous. The aggregated losses emanating from the multiplicative crimes committed using stolen documents commonly referred as identity fraud are even bigger. Identity fraud covers a wider set of crimes, all of which have stolen documents as the common thread. The stolen identity documents are used to misrepresent the identities of those about to commit crime and to make it easier to evade detection and punishment from law enforcement agencies (Smith 1999).

A major investigation in the United Kingdom by the cabinet office found that *identity fraud is an important and growing problem linked to organized crime in a*

number of forms (Economics and Domestic Secretariat 2002). The cabinet report goes on to note that identity theft is almost always committed as a first step in a chain of criminal acts.

Thus, identity theft is not only a problem because of direct losses, but also because of the myriad other crimes that it is feeding. The various forms of identity fraud-related crimes are forecast to reach $2 trillion dollars by the year 2005 (Aberdeen Group 2003). Even more disturbing is the new trend in which identity fraud has moved away from a petty thief's small-scale operation to a large-scale organized crime.

1.2.4 Role of Emerging Technologies in Increasing Identity Fraud

The most common examples of identity fraud include credit/debit cards, checks, telephone cards and social benefits fraud (U.S. Federal Trade Commission 2004). A closer look at these different types of identity fraud shows that the domains of application are different, but the criminal methods used are similar. In all cases, the offender either open new accounts using stolen documents (true application fraud) or takes over the victim's existing accounts (account takeover fraud).

Identity fraud is both an online and offline problem. In the past, the biggest component of identity fraud was conducted offline. Family members and friends carried out the identity fraud. Petty thieves rummaged through garbage bins looking for personal information that could be used to create false identification documents. They redirected mail from victims' addresses to sanitized addresses to obtain credit card numbers and other identifying information. This mode of identity documents acquisition is still going on. However, recent trends indicate that online identity fraud is becoming the more

dominant fraud, having moved from 42% to 55% of total identity fraud between the years 2001 and 2003 (U.S. Federal Trade Commission 2004)

Organizations have improved their methods of dealing with offline fraud and so that the rates have now declined to levels of less than 0.06% of gross sales (Cheney 2003). On the other hand, a survey of online fraud with credit card companies, reports that online fraud still constitutes about 1.7% of total sales. This transforms to about $1.6 billion in losses (CyberSource 2004). This occurs even when these companies are rejecting about 8% of their orders on suspicion that they are fraudulent. Since some of these orders are valid, the companies also suffer an opportunity cost from the missed sales.

There is an increased reliance on manual reviews (up to 23% of all online orders), which leads to increased staff. Identity thieves would rather avoid appearing physically at a primary financial institution where a teller can use an account holder's picture, signature or other recorded identification verification to detect fraud. A thief would rather shop online or make monetary transfers online. This is because the identity thief is aware that it is more difficult to fight online fraud for reasons of anonymity, traceability, lack of jurisdiction, volatility of evidence, etc. (Australasian Center For Policing Research 2000). Thus, the Internet offers a better alternative for identity fraud with more convenient transactions and less potential for being caught. Unless better protection is given for online authentication, identity fraud can be expected to continue to rise since the rewards are high and the risk is low.

1.2.5 The Impact of Identity Fraud

Consumers are, by law, protected from direct fraud losses but still can spend an enormous amount of time (over 300 million person hours) and indirect costs (over $5 billion) recovering from their losses and damaged reputations (Synovate 2003).

Merchants have to meet the direct losses of over $279 billion annually (Identity Theft Resource Center Inc. 2003) and have to pay high insurance premiums to compensate for anticipated identity fraud losses. This cost is passed on to the consumers in higher prices for goods. Companies can also experience a damaged company image, after security breaches resulting in theft of personal identifying information, is published in the media. Such loss of corporate image eventually results in decreased investor's confidence, falling share prices, customer defections and litigations. These companies are also rejecting about 8% of total sales orders on suspicion that they are fraudulent. Since some of this orders are valid, this then becomes an opportunity loss for the missed business (CyberSource 2004).

The government also loses financially because it has to deal with increased spending on social programs such as social security as some identity fraud involves impersonating the true recipients of these benefits. Governments also need to meet increased costs because of the increased policing budget needed for law enforcement agencies. This cost is passed to the citizen in form of increased taxes or reduced benefits. This reduces the working capital from the private sector which is the main driver of economic growth engine. It also reduces the consumer's purchasing power resulting in reduced product demand. Thus, everyone is significantly affected by identity fraud (RSA Security Inc. 2003).

Although Section 1.2 presents a strong argument that identity fraud is major concern for developed countries in the world, this dissertation does not focus on the types of fraud or its trends. The purpose of presenting the above discussion is to give motivation for the work in this dissertation, which is to investigate the feasibility of a keypad biometric for user authentication. The fact that identity fraud is moving increasingly online suggests that online data entry may be a useful point to focus on for developing prevention methods. The fact that identity fraud is so large suggests that any solution, however, small its application, will be likely to have significant benefit.

1.2.6 Issues Responsible for Rising Identity Fraud Problem

The first part of this chapter demonstrated that identity fraud is a serious problem with enormous cost to the individuals and business organizations. Several researchers and government agencies have attempted to address the problem with various degree of success but the problem remains unresolved. The following are some of unresolved issues leading to rampant levels of identity fraud from previous work.

More awareness is still required. The full threat potential of identity fraud is still unrecognized with traditional crimes like drugs and homicide still being perceived as more serious hence getting higher priority (U.S. General Accounting Office 2002).

The credit card companies, in response to the cut-throat competition in their line of business have relaxed the identification, vetting, and verification procedures. Most applications are approved instantaneously based on the provided information without authenticating that the applicant is the true owner of the provided information (Givens 2000).

Credit card companies send unsolicited pre-approved new cards with activation instructions to potential customer addresses. Such cards are easy targets of identity thieves (Givens, 2000). The law enforcement agencies did not recognize the full damage potential from identity theft before it got out of control. Good security and identity management systems come at a price. Most organizations have not put the appropriate investment in identity management systems. Some of the loopholes exploited by fraudsters can be sealed off easily. However individuals and organizations are still resistant to change their old security habits. Several of the top managers are not aware of the vulnerabilities of the systems they are using.

Most of the solutions for combating identity fraud involve gathering of human data. This raises several genuine privacy issues (Gordon and Willox 2003). There are several agencies and institutions combating the identity fraud problem. However some are duplicating each other's work or reinventing the wheel. They are not leveraging the existing databases, reports and other resources in solving identity fraud (U.S. General Accounting Office 2002). The protocols for dealing with identity fraud cases that crosses different countries are still unclear. More collaboration is still required between the crime fighting agencies.

Organizations are using firewalls and anti-virus systems at the perimeter of their systems to protect themselves against outsiders. This is important but even more important is protection against insiders. Research shows that the biggest threat normally comes from the insiders (Shaw et al. 1998). The introduction and use of social security and driving license numbers as primary keys in general databases without a thought out plan on the control of who gets access to what has increased the exposure points of such

data to unauthorized parties (Givens, 2000). The introduction of the Internet, pervasive technologies, and high-resolution duplication equipment has made a bad situation worse. It is no longer possible to say with certainty that the person on the other side is really the genuine person. The Internet has availed easier methods of transacting in stolen identifiers and identification documents. The high-resolution, full color printing and copy machines have made forging of identification documents from stolen identifiers easier.

Most businesses and organizations still use the simple password authentication system, which can be compromised using easily available tools. Identity fraud will only be mitigated by a multi-faceted approach of applying multiple solutions. However, there are no concrete standards or frameworks on the integration and portability of such different products and solutions.

The rest of this dissertation will focus on only one of these issues, that is, the issue of inadequate authentication.

1.3 Problem of Inadequate Authentication

The objective of this dissertation was to develop and evaluate a transparent and secure solution for mitigating identity fraud at the human-computer interface. The method solution selected was the development of an authentication method that used the personal biological behavior of each individual, in this case the person's typing patterns. The next paragraphs support why this approach was taken.

There are several outstanding issues that make identity fraud rampant several of which were given in the previous section. However the most critical problem is

inadequate authentication systems. The fact that an identity thief can take someone else's identifiers, and pass through the authentication systems without being detected is a manifestation of the inadequacies in the current systems and processes.

The current authentication systems have two key problems. The first of these is the localization of the identification systems. Identities are often easily copied because their verification data is local, e.g. it is easy for thieves to order credit cards in someone else's name, change their address, and use that person's good credit history because there is lack of cross checking of house sales, tax records and vehicle registrations. This dissertation will not address this problem.

The second problem is the use of external identifiers like the tokens (e.g. magnetic cards) and knowledge-based systems (e.g. passwords). Magnetic cards can be easily scanned and counterfeited. Smart cards have higher data carrying capacities and are harder to counterfeit, but they can be broken using ionizing or microwave radiation (Smith 1999). The passwords suffer from the *good password dilemma*; if the passwords are easy to remember, then they are also easy to crack. If they are difficult to crack, then they are difficult to remember and the user invariably writes them down where they can be stolen. This explains why about 80% of all network intrusion problems are caused by bad passwords (O'Gorman 2004).

1.4 Dissertation Problem Statement

The above arguments lead to the key problem of this dissertation, that is, the development and investigation of a keypad biometric as a user authentication method. The rest of this dissertation will therefore focus on (1) the development of such a biometric, and (2) the

investigation of the feasibility of the biometric developed. This investigation will be twofold. First, an experiment will be run to determine how well the developed method works for a variety of possible real world situations that such a biometric might be used in. Second, user interviews and surveys will be run to determine how acceptable the biometric method is to the typical users that might be adopting the technology. Thus, the dissertation is a presentation of a methodology to employ for the development of a new technology that has both accuracy and user invasive characteristics.

1.5 Dissertation Structure

The dissertation is organized as follows. This first chapter discussed the motivation for developing a better authentication method.

Chapter 2 analyzes the current methods of authentication and their shortcomings. A solution to the problem is suggested as addition of a biometric layer to the present identifiers. A Keyboard biometric is shown to have the potential of being a possible implementation of the suggested biometric solution. Previous work on keyboard biometrics and pattern recognitions systems is reviewed to set the basis for several design decisions taken in the development of the biometric keypad. This is followed by a review of technology acceptance and adoption literature with the objective of understanding the important issues in the acceptance of the biometric keyboard technology. Several gaps in the technology acceptance literature are identified and solutions sought from the biometric literature. Chapter 3 introduces two research questions. The first research question is on the technical feasibility of developing the biometric keyboard while the second research questions investigate the critical factors that would be important in the

acceptance of such a solution. The Chapter ends by presenting the road map that was used to answer the two research questions.

The next three chapters describes various aspects of the investigation on research question one. Chapter 4 investigates the technical feasibility of the biometric keypad and explains the rationale and design of the biometric keyboard prototype and the associated classifiers design. The chapter then presents the findings to show the feasibility of the biometric method. Chapter 5 gives the design and methodology followed in evaluating the biometric keyboard prototype. This includes the operationalization of variables and the experimental procedures. Chapter 6 describes the analysis and results for the evaluation of the biometric keypad.

Chapters' 7-10 addresses research question two. Chapter 7 gives the research methodology that was followed in the executive interviews using grounded theory approach. This is followed by the analysis and results of the executive's interviews in chapter eight. A biometric acceptance model is formulated and six hypotheses proposed. Chapter 9 presents the research methodology followed in designing and administering the user survey while chapter 10 gives the results of the user survey including acceptable parameters for the biometric ATM and the validation of the biometric model.

Chapter 11 starts with discussions of results from each of the three studies. An overall discussion follows in which the connection between the different chapters of the dissertation is demonstrated, to show that the whole dissertation is coherent and parsimonious. A summary of the contributions and limitations of the three studies follows. Finally suggestions are given for future research with the goal of extending several findings from this dissertation.

1.6 Summary

This chapter provided motivation for the research undertaken and support for the particular solution chosen. The advances made in information technology were shown to be beneficial but to have also resulted in increased fraud. Support was given for the proposed solution of using a keypad biometric for authentication. The key problem of the dissertation was then defined, that is, of developing and investigating the viability of a keypad biometric for improving user authentication. Finally, the structure of the rest of the dissertation was given.

The next chapter will build the theoretical support for the work that is undertaken in this dissertation. It will define key terms used in the dissertation and then develop research arguments from prior research that has been done in this area to support the research questions being posed in Chapter 3, the prototype design decisions taken in Chapter 4 and the studies described in Chapters 5 through 10.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Overall, the emphasis of this dissertation is to investigate the feasibility of a biometric method for mitigating identity fraud. As such, there are multiple factors to consider in this feasibility analysis. They include detailed factors that affect the design and reliability of the biometric method, but also large scale factors that affect its placement in the world, that is, the engineering and business model that might be selected to bring about its introduction. Thus, the literature used in this chapter to support the approach taken represents an overall model of how to approach the design, development and introduction of a type of product that can be expected to have performance and social implications.

This chapter starts by giving precise definitions of terms that will be used throughout the dissertation. It then presents a review of current methods used to identify and authenticate humans with a discussion of the shortcomings of the approaches taken. Possible solutions are proposed in the biometric area. Although other biometric technologies are viable, the work focuses on keyboard-based authentication as a viable technique to explore. This is because the keypad is simple, pervasive and inexpensive.

Previous research on keyboard-based authentication is discussed and pressure is proposed as an additional metric that might obtain better results. An overview is given of the pattern recognition techniques that will be employed to develop the keyboard-based biometric algorithms with the plan to present a more detailed reasoning for the choice of the methods in Chapter 4 which describes the prototype development.

Following the literature support for the development of the biometric method is a section on the psychology of typing behavior. This discussion cites papers that describe what is known about human keying behavior and skilled performance acquisition. These papers provide the theoretical basis for the experiments described in Chapters 5 and 6 of the dissertation. These experiments are run to investigate the impact on performance that human variance might cause in the use of the biometric technology, in short, the feasibility of the proposed biometric in the everyday world. Finally, a review of technology acceptance literature follows since it is not just performance but acceptance that makes a technological innovation successful. The chapter ends with a review of those critical factors that have been uncovered in previous studies that are likely to determine the acceptance of biometric keyboard systems.

2.2 Shortcomings of Current Authentication Methods

Human identification is defined as the *association of data with a particular human being* (Clarke 1994). The goal of this identification in computing is to determine whether the person logging in is one of the known members of a database of legitimate users. This is accomplished by searching the central database for a template that matches the user log-on-template. Authentication is different than identification. The goal of authentication is to verify that the person logging on is who she or he is claiming to be, and not an imposter. Comparing the logging-user-template with a template that was acquired during registration and currently stored in the database accomplishes this objective.

There are three common identification methods, namely, token-based, knowledge-based and biometric-based methods (Polemi 1997). Token-based

identification systems use something that the user has as a form of identification. Common examples include magnetic strip cards and smart cards. Knowledge-based identification systems use an identifier that is known only to the individual in question. Examples include passwords, personal identification numbers (PINs), challenge questions etc. Biometric-based identification systems identify individuals based on some measure which is unique to each person, and carried on that person as part of their biological entity. The biometrics used can be the person's physical features (physiological biometrics) or based their behavioral performance (behavioral biometrics). Physiological biometrics includes appearance (height, skin color, eyes, photographs etc) as well as physiographic characteristics such as facial analysis, fingerprints analysis, retina scanning, vascular patterns, hand geometry and DNA-patterns (Clarke 1994). Physiological biometric have high accuracy rates due to continued years of research. Behavioral biometrics involves identifying humans using their behavior. Common application includes voice characteristics dynamics, signature dynamics, keystrokes dynamics, mouse stroke dynamics and click stream dynamics. Most of these technologies are in their early years of research.

A pertinent issue in managing authentication is one of catching the imposter at the entry attempt. Issues with human nature form the weakest link in this process. The human element needs to be appreciated if the weaknesses of the current methods are to be fixed.

Token-based authentication systems suffer from tokens getting into the hands of the wrong person, and thereby compromising the entire system's security Knowledge based systems suffer from the limitation that the knowledge needs to be memorized and

has the risk of being forgotten, or shared hence can be compromised. The commonly chosen passwords are names or birth dates of members of the immediate family. Identity thieves can easily crack such simple password schemes with easily available programs. The web has several mushrooming family tree search engines which can work out the common family lineage to get a common name set for first line of attack against the password systems. If such first line of attack fails, then the offenders can use programs with brute force algorithms.

Organizations have tried to overcome the problem of simple passwords by forcing the users to use computer generated hardened passwords. However, such passwords are hard to remember and the user ends up writing the password on note pads which are then stuck on the front of the computer. Acquiring such passwords will be an easy task for those with a criminal mind. Identity thieves have been known to stand behind customers on ATM lines and note the used personal identification number. Others use social engineering methods to extract the knowledge from the genuine but trusting owners.

The public/private key encryption systems reduced some of the knowledge based systems weakness. However there will always be the problem that if the private key gets into the wrong hands then the whole system will be compromised. What the public key system does is to reduce key sharing. This in turn reduces the risk of compromising the private key but the risk is still there.

What is required is a one-password solution that is live and inseparable with the individual and one that does not have to be shared. This will minimize the chances of being compromised.

2.3 Choosing a Biometric to Supplement Current Authentication Methods

This dissertation suggests that a possible solution to the shortcomings of knowledge and token based systems is to add a biometric layer to the existing layer of external identifiers in a two or three factor authentication. The rest of this section investigates applicable biometrics.

The section starts by presenting the architecture and operation of biometric systems so as to have a common yardstick for comparing and choosing the most appropriate biometric for a specified need.

Biometrics can either operate in enrollment mode or in authentication mode (Jain et al. 2004). In the enrollment mode, the specific user template data is captured and after labeling is stored in the availed database. The next time the user attempts to log in, the new template is compared with the template in the database and the user is authenticated if both match.

The common modules of a standard biometric system include the (1) sensor module which is the input data reader, (2) the ***feature extraction module*** which extracts the features that will be used for comparison, (3) the matching module which compares the user template with that in the database, and the (4) decision making module which makes the final decision on identification or authentication.

2.4 Types of Biometrics

There are several biometric systems several of which will be considered in this section. *Finger print* identification depends on the fact that different individuals have unique fingerprints. It is a well-developed and accurate technology. It is the most widely used

and accepted biometric (Reid 2004) used widely. However it has a slight association with criminality from its years of usage by criminal enforcement agencies. Finger print identification methods use either the macro features of the finger print like the ridge patterns , type of line etc while other methods use the micro features like the minutia points (Reid 2004). Typical equal error acceptance rates of 0.1% and 0.37% have been obtained for optical and capacitive systems respectively (Albrecht et al. 2003)

Iris recognition is one of the most accurate methods. The iris meshwork of connective tissues is unique for every individual. It cannot be changed even by surgery. It can also be registered unobtrusively. However it has not been socially accepted. This is mostly because of its use of infrared beam, which raises the fears of medical side effects (Polemi 1997).

Retina scan depends on the fact that the blood veins at the back of the retina are unique for different individuals. The system is highly accurate and the retina veins cannot be changed by surgery. However the systems are quite expensive. They are also highly invasive (Polemi 1997).

Facial analysis depends on the fact that different individual face characteristics and position of the nose, shape of the eyes, chin; eyebrows and the mouth are unique. There has been a lot of research in the field in the last couple of years. The systems are reasonably accurate. However they only work well for still pictures and straight frontal face pose. They do not respond well to face rotations. Further the systems are still very expensive and proprietary. They are also mostly based on neural network which takes a long time to be trained (Polemi 1997).

Hand geometric depends on the fact that the hands, palms, finger size and geometry and finger prints for different individuals are unique. The systems are generally fast both at enrollment and at verification. However they don't work well if the hands are rotated which makes then inconsistent in field conditions. They also do not work well if the individual have swollen fingers, are wearing rings. A fake replica of the human hand can also fool the systems (Polemi 1997).

Speech analysis method depends on the fact that the combination of sounds, phonetics and vocals for different individuals is unique. It is difficult for the computers to faithfully analyze and differentiate the different voice characteristics. Thus the method is not as accurate as the physiological biometrics methods. The accuracy also gets highly affected by changes in user's voice due to sickness or to background noise (Polemi 1997). However this is one technology that would be very appropriate in fighting telephone identity fraud once it has matured.

Hand written signature depends on the fact that signing up is a reflex action, which does not depend on deliberate muscle motor control. Thus a combination of the rhythms, successive touches, velocity and acceleration are unique for different individuals. The systems are accurate. They are well accepted by the society, as they are similar to the traditional paper signature. However they do not respond well to people who change their signature rapidly. Their acquisition costs are high and proprietary hardware is required (Polemi 1997).

Keystroke analysis depends on the fact that the keystrokes duration, inter-keystroke times, error frequency and force strokes are unique for different individuals (Monrose and Rubin 2000). The method can either be static where the user is identified

at log in or they can be dynamic where the user is being constantly being monitored and authenticated as they go about their normal typing business. The method is simple, cheap and convenient. The method utilizes most of the existing hardware and software in computer equipment and can be done covertly if need be. It can be implemented in software hence do not need any extra hardware. Keyboards are cheap and transparent to the user (Ord and Furnelli 2000). However the effect of hand injury, fatigue and stress are not well understood. Thus the method seems very promising for use in combating identity theft as it can be used in the background and does not need any special hardware or software. The goal of this study is to learn more about its capabilities and limitations.

2.5 Evaluation of Biometrics Technologies

There are several issues that are important in evaluating the performance and suitability of a biometric. The issues can be grouped into engineering issues, management issues and user issues.

2.5.1 Engineering Issues

The engineering issues are important to designers of biometrics in helping design a product that will have the required functionality. These issues are the basis of the first study on technical feasibility. This subsection discusses some of the important engineering issues in biometrics

Performance of a biometric system is highly dependent on its accuracy. Biometric accuracy can be hindered by two types of errors namely false rejection rates (FRR) and false acceptance rates (FAR). FAR is the probability that an impostor will be

falsely accepted as a legally registered user. FRR is the probability that a legally registered user will be falsely rejected by the biometric system when presenting his or her biometric feature (Graeventiz 2003). The objective of a given biometric is to have the least FAR. However, reducing false acceptance rates increases the false rejection rate. This translates into increased rejections of the genuine user which is frustrating and makes the biometric systems more difficult to use. The normal solution is to decide on a compromise that is acceptable to all the stake holders.

In order to have high performance, good identifiers should be unique but universal. This means that each individual should only have a single identifier, which should be different from that of any other individual. This is the most fundamental tenet that human identification systems depend on (Clarke 1994) . This will be addressed in the biometric keyboard by investigating the technical feasibility of discriminating different individual using their typing patterns.

The human patterns should be stable over time or ideally permanent (Clarke 1994). The patterns recognition systems which are used for identification and authentication work by learning a model from the training data during enrollment and using this model to later determine if there is a match with a user-log-in template. If the new data is different from the one learnt during training, then this will lead to deterioration in the performance of the biometric. This will be addressed in this study by longitudinally investigating if the keystroke typing patterns will change over time.

The other important aspect of engineering for a biometric is the issue of security. Biometric systems are not foolproof but can be compromised by an attacker. In particular, users feel that the biometric patterns from the genuine use can be stolen and

used by impostors to the detriment of the genuine user. Biometric systems can be compromised either by direct attack, by spoofing or by replay attacks. This dissertation suggest that one of the ways of strengthening keypad biometric is by including pressure features so that there are multiple group of features to help in discriminating especially for cases where there is high correlation or similarity between two user patterns.

Scale is a very important element from an engineering point of view. This refers to the ability of a biometric system to maintain good performance as the number of users increase. A good biometrics' performance should gracefully withstand increasing number of users.

2.5.2 Management Issues

Biometric management issues refer to those issues that help make the deployment of biometric smooth. The first issue is manufacturing. The chosen biometric system should be standardized and supported by the mainstream manufacturers. It should also be interoperable with current computer hardware and software (Clarke 1994).

The biometric identifiers being used should also be universal. This means that every individual from the total population should have such an identifier. If such a biometric is not universal, then there should be a backup method that can be used by a disadvantage person who does not have the biometric in question. Thus some people may have lost their thumb finger and it is the responsibility of the management to see that there are provisions for such an occurrence

2.5.3 User Acceptance Issues

To increase the acceptance of biometric technology, several aspects of user friendliness should be addressed (Albrecht 2002). One such issue is ease of use.

The biometrics should be easy and convenient to use with minimum time for enrollment, identification, and verification. The biometric should have minimal false rejection which is a nuisance to the users. The measurements taken by the biometric should not inconvenience the subjects and should not take too much time. This will be addressed in this dissertation by finding the acceptable number of trials that a user would be willing to repeat typing the patterns. Ergonomics is very important; the goal should be to authenticate users in their natural position and while in their every day motion (Albrecht 2002).

The identifiers should conform to the limits of social and ethical acceptability and should not be overly intrusive. Privacy can be looked from two perspectives (Cavoukian 1999). The first perspective is that of the privacy of the person. Biometric by design can identify the owner of a given pattern. This can be abused to covertly identify and monitor users going about their business without their express authority and without them being aware that they are being monitored and identified. Thus a good biometric should not be intrusive. People also have the fear that biometric technology will be used to monitor their movement by the government – one of the fastest growing applications of biometric is in airports, immigration – antiterrorists. The second perspective is that of the privacy of the data. There is concern that on the privacy of the data captured by the biometric system. There is fear that the system may be collecting other private

unauthorized private data, may be collecting unnecessary data or may be using the data for other unintended purpose (Cavoukian 1999).

2.6 Selection of a Potential Biometric Technology

A comparison was done among existing physiological and behavioral biometric methods, namely the fingerprint verification, retina scan, iris scan, face recognition, hand geometry, speech analysis, handwritten signature verification and keystroke analysis method.

The finger print method is very accurate although associated with criminality by some people. The iris recognition method is very accurate, but has acceptance problems. The facial analysis method works well but is sensitive to facial angles and lighting. The hand geometry method is accurate and well accepted, but expensive. The hand written signature verification is also highly acceptable but not as accurate (Polemi, 1990). All of these methods are hard to implement in online systems. Speech analysis is mostly appropriate for voice-based systems. The final conclusion was that the keystroke dynamic method has the potential of being most appropriate for the needs of this study. This method is simple, cheap, convenient and transparent to the user. Keyboards are also commonly available and need not be online to be used. An added advantage is that unlike most of the other biometric systems, the keystroke identification pattern can be changed in case the first one is compromised.

2.7 Uniqueness of Individual Typing Patterns

This section demonstrates by citing other studies that keying generates a completely unique typing pattern for each user. . It discusses the key pattern classification work that has been done to date and then suggests parameters that can be added to the classification algorithms to improve classification and thus, authentication, further. Thus, the latencies between successive keystrokes, keystrokes, durations, finger placement and applied pressure on the keys can be used to construct a unique user signature/profile (Monrose and Rubin 2000).

Gaines et al. (1980) measured keystroke latency times for a succession of keystrokes from seven secretaries typing one set of three passages of text, and retyping the same three passages after four months for comparison. They were able to identify each secretary reliably (FAR = 0%, FRR = 4%). However the shortcoming of their experiment was that they used too few subjects. Leggett et al. (1989) extended Gaines work to include more subjects and longer text (FAR = 5%, FRR = 5.5%). Mahar et al. (1985) went a step further by better outlier detection and the elimination of pooled variance. Garcia (1986) patented a method that used mean latencies to form an electronic signature but did not report FAR and FRR statistics. Young and Hammon (1989) patented another method, which could use time and pressure, but the implementation details are not given. Joyce and Gupta (1990) integrated the existing works to come up with a simple but elegant classifier using key digraphs (FAR=0.25 % FRR= 16.7%). Monrose and Rubin (2000) improved the sample replacement methodology used by Joyce and Gupta and obtained identification rates of 83.2%, 85.6% and 87.2% with the Euclidean, non-weighted and weighted Bayesian classifiers respectively. Obaidat and

Sadoun (1997) computed digraph similarities using k-means, cosine, minimum distance, Bayesian and potential function algorithms with the inter-key times, key-hold times and their combination. The best identification accuracy of 100% was achieved using combined hold and inter-key time using a fuzzy network solution. Bleha et al. (1990) used a Bayesian minimum distance classifier (FRR= 8.1%, FAR= 2.8%). Bergadano et al. (2002) suggested a new method that measures the degree of disorder between two typed samples with authentication occurring only if the distance between the two samples is below a certain threshold (FAR = 4%, FRR = 0.01%). The keystroke analysis method has been recommended as a second layer of security. To support this approach, a learning algorithm was developed by extending Lempel-Ziv compression algorithm with time latencies to get accuracies of about 97% (Mordechai et al. 2003).

All of the above studies use time latencies. Further they share a common approach of using a lot of text before arriving at an authentication decision. However in real life, especially the identity theft scenarios, the user will only type a single user name or PIN on a keypad hence there is a need to improve the above approach so that it can work for a regular PIN which is usually 4 digits. Yu and Cho designed a support vector machine that used password strings ranging from 6-10 character strings (FRR =3.54, FRR=0) with twenty one subjects. Ord and Furnelli (2000) used a neural network approach to develop a keypad authentication system (FAR= 9.9% FRR= 30%). However they only used time latencies. To improve such authentication results, there is need to include both pressure patterns to the time latencies patterns with the goal of getting more discriminative and resilient identification.

2.8 Gaps in Previous Work in Biometric Keyboards

There are several gaps in previous work on keystroke analysis. The first shortcoming is that most of the reviewed studies used time latencies only. This study will use both pressure and time latencies. (2) The second shortcoming is that most of the studies concentrated on free keyboard typing. The current authentication systems are using keypads with four or six character PINs hence there is a mismatch between what was done in the studies and the reality. An exception to this are the two studies keypad studies (Kotani and Horii 2002; Ord and Furnelli 2000). The third shortcoming is that all of the research that has been done in developing biometric keypad classification algorithms has not examined the large number of external parameters that can affect classification in day to day usage. In particular human variability is likely to make a large difference. The next section discusses this variability in terms of keying patterns. Other sources of variability include user responses in different temperature situations, the impact of stress on the keying pattern,, the effect of other packages a person may be carrying, etc.

2.9 Developing a Keyboard-based Classifier

There are decisions that need to be made in the design of the prototype biometric keypad that can be based on a large amount of previous work. Such decisions include the choice of the classification features and the choice of classifiers. The next subsections give the background and the rationale to support this decision-making. The first section presents the rationale for choosing to use time and pressure characteristics of the keystroke patterns. The section also elaborate of the specific characteristics of the time patterns

used and the choice of wavelet coefficients as the best classification feature for the pressure aspect of the typing pattern. The section ends with the short listing of the best classification method as neural networks and support vector machines from the previous literature.

2.9.1 Choosing the Time Features to Use for Classification

The first decision to be made was what type of features to use for classification. There were several candidate features and the performance of the classifier will partly depend on the choice of the classification features hence the need for prudence.

The original work in keystroke dynamics suggested that the digraph latencies between successive keystrokes can be used to create an individual signature. The digraph latency time is the time between two adjacent digits or letters. Leggett and Williams (1988) developed a method that used the digraph latency to differentiate between different users. They attained accuracy rates of 5% FAR and 5.5% FRR. The digraph latency time can be broken down into two components. These components are the key-down-time and the inter-key-time. The key-down-time is the time that a certain key is pressed down while the inter-key-time is the time between the first key release and the second key depression. Research has shown that using the key-down-time and inter-key-time is better than using the digraph latency time (Napier et al. 1995).

Thus a decision was made in this dissertation to use the key-down-time and the inter-key-time as the time classification features with the aim of attaining optimal results.

2.9.2 Decision to add Pressure as a Classification Feature

The norm in previous keystroke analysis work has been to use time-based features. Reasonable classification rates were attained as earlier given in previous section. One of the major shortcomings of the previous work was the use of too much text. The amount of text used needs to be reduced. However, reducing the amount of text reduces the power of discrimination. This results in a conundrum, which is hard to break. One of the ways that such a conundrum can be broken is to look for additional features that can be incorporated to boost the discrimination power. One such solution can be found in a patent by Young and Hammon (1989). In this patent, the inventors suggest that addition of pressure to the time features can improve classification power but did not explore how pressure might be added. More recently, Kotani and Horii (2002) explored this proposal of adding pressure to the time features. They used a numeric keypad with pressure sensitive resistors to conduct a longitudinal study with five subjects over a one-month period with subjects entering a four digit PIN. They found that pressure significantly improved their discrimination results. Kotani and Horii's work demonstrates that pressure adds discriminative power. This dissertation will therefore add pressure to the time latencies to make a more discriminative and resilient identification. The dissertation will also extend the exploratory study by Kotani and Horrii (2002) and examine the performance of such a biometric keypad under various external parameters that can affect classification in day-to-day usage.

2.9.3 Choice of Pressure Wavelet Analysis Method

The previous subsection justified the decision to include pressure as an additional feature to boost classification. However, there are several pressure characteristics that can be used. A decision needed to be made on the exact feature that had to be extracted from the pressure signal.

The goal of feature extraction is to acquire the best characteristics from a signal that can be used either for representation or for classification. The geometric characteristics (e.g. height) of the pressure signals were the first candidate feature for pattern classification. However, the geometric features suffer from noise distortions and subjects may apply different pressure at different occasions. A better alternative is to perform a mathematical transformation of the pressure signal to the frequency domain so as to get more signal information that is not readily available in the time domain. This led the study to Fourier transformation. A Fourier transform decomposes a signal to complex exponential functions of different frequencies defined by equation (1) below.

$$F(\omega) = \int_{-\infty}^{\infty} f(t) e^{-j\omega t} dt \qquad \textbf{Equation 2.1}$$

Where t = time, ω = angular frequency function

However the Fourier transform will only decompose the time signal into the frequency component without giving any information of the time position (the time an event occurs or the difference in time between two event occurrences) in which the frequency components are appearing. The later is very important for non-stationary signals like the keystroke signals. A decision was made to shift to wavelet analysis to overcome the shortcomings of Fourier analysis.

The wavelet transform extends the same idea of the Fourier series but overcomes the above shortcoming by performing a mathematical transformation that retains both frequency (scale) and time (position) information. The wavelet convolutes the original signal with a basis function called a ***mother wavelet*** The mother wavelet used in this dissertation was ***Haars*** The later translated (position shift) and dilated (scale) the signal as per the following equation (Misiti et al. 2004).

$$C(\text{scale, position}) = \int_{-\infty}^{\infty} f(t)\Psi(scale, position, t)dt \qquad \textbf{Equation 1.2}$$

Each convolution results into a set of wavelet coefficients dependent on the mother wavelet. The signal is repeatedly decomposed into a coarse and a detailed information portion by passing the signal through a series of high pass and low pass filters. The low frequency component (approximation) is what gives the signal the basic identity while the high frequency component (details) gives the signal the fine aspects. The wavelet coefficients for high and low frequency portions are down-sampled to keep the total number of coefficients constant (Misiti et al. 2004).

The diagram below demonstrates the convolution of a signal into wavelet coefficients. The original signal is decomposed into two portions labeled as CA1 and CD1. CA1 is the low frequency portion (approximation) while CD1 is the high frequency portion (details). The same process is repeated again for each of the two portions until the minimal level is attained.

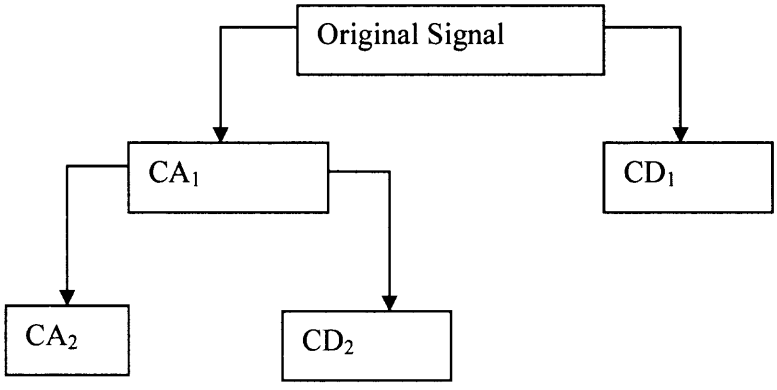

Figure 2.1 Wavelet decomposition diagram

The minimal level of decomposition can be determined either empirically or using entropy methods. The minimal level in this dissertation was determined empirically as explained in Chapter 4. Thus the choice of the wavelet method was made because of the superiority of the method in giving complete aspects of both the frequency and time position of a signal and also in part, because of the popularity of this method in current pattern recognition literature where it has been shown to work in a large variety of situations (Misiti et al. 2004; Pitter and Kamarthi 1999).

2.9.4 Choice of a Classifier

Authentication requires a comparison of a stored set of patterns with an incoming set of patterns to verify that the new set, albeit somewhat different, can only be generated by the person who generated the stored set of patterns. Thus, authentication is a pattern classification problem. The goal of any pattern recognition system is to produce a model that can predict the class labels of some unknown patterns after being trained on a set of known patterns.

Most of pattern classification problems require a classification of a waveform or geometric figure. The original signal is expressed as a random vector in an n-

dimensional space. Pattern classification then involves finding the boundaries between two or more distributions by estimating the density functions in a high dimensional space and dividing the spaces into the regions of the categories or classes (Fukunaga 1990)

A Bayes classifier would be the best classifier because it gives the minimum probability of error. However the Bayes classifier requires knowledge of prior classification probabilities which are not always known. The second choice was to use a parametric classifier like the linear, quadratic, or piecewise classifiers. Parametric classifiers assume that the mathematical forms of the distributions are known or can be assumed which was not the case in this dissertation. Previous work on comparison of different classifiers has found that neural network and support vector machine methods are among the most versatile classifiers (Hsu et al. 2003).

This study used the above work to narrow down the search for an appropriate classifier into either a neural network or a support vector machine classifier. The next two subsections give the background on the design of neural networks and support vector machines. This background will be used in Chapter 4 in the implementation of the neural network and support vector machine classifiers.

2.9.5 Design of Neural Network Classifiers

This section summarizes the working of neural network. A full description can be found in Duda et al. (2000)

The neural networks are made up of a cascade of discriminant functions (a function that can be used to different two or more classes).

A discriminant function can be written as

$$g(x) = w^t x + w_0 \qquad \textbf{Equation 2.3}$$

Where **w** is the weight vector and W_0 the bias or threshold weight.

The figure below shows a possible implementation of such a linear discriminantt function having d-inputs.

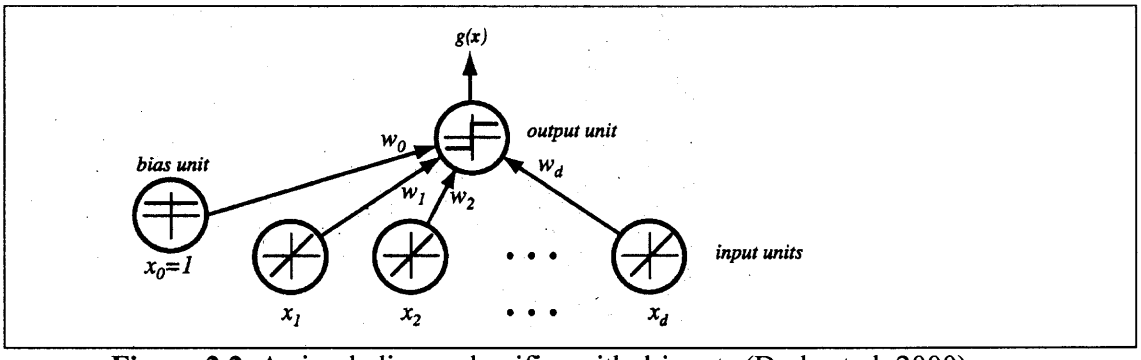

Figure 2.2 A simple linear classifier with d-inputs (Duda et al. 2000)

A two category case will implement the following decision rule (Duda et al. 2000)

Decide ω_1 if $g(x) > 0$ and ω_2 if $g(x) < 0$

Thus $g(x) = 0$ is the decision boundary (called a hyper plane for the linear case) that separates the two classes.

The output of the discriminant function is the sum of the products of each input feature multiplied by its weight and is represented by the following equation for the general case.

$$\mathbf{g(x) = w_0 + \sum_{i=1}^{d} w_i x_i} \qquad \textbf{Equation 2.2}$$

The linear discriminant function works by constantly adjusting the input vector weights to match the known class labels during training and later use the resulting

function with adjusted weights to classify new data into the appropriate classes during testing. However, real world cases consist of many non-linear cases hence the need to extend the working of a linear discriminant functions. One possible way to do this would be to multiply the discriminant function with a non-linear function. But it is hard to predict which discriminate function to use upfront. Neural networks solves this dilemma by learning the nonlinearity of the data at the same time that they are learning the linear discriminate function from the training data. Multilayer neural networks (MLPs) implement several layers of the linear discriminant functions to produce optimal non-linear classifiers which are extremely powerful (Duda et al. 2000).

2.9.6 Design of Support Vector Machine Classifiers

Support vector machines are a relatively new method of pattern classification compared to other methods like neural network classification. The method is powerful and has been shown from previous research to outperform most of the other pattern recognition methods (Cortes and Vapnik 1995). The goal of the SVM classifier in this dissertation was to produce a model that could be used to predict the owner of a given typing pattern.

Linear learning machines are simple to design and operate. However they can only separate linearly separable cases and have strong limitations when the problem is non-linear. Most real world problems are non-linear. SVM overcomes the shortcomings of linear learning machines by using kernel functions to perform a nonlinear mapping of the problem. The input data is transformed into a higher dimensional space in which a linear learning methodology is then applied (Cristianini and Shawe-Taylor 2000). The reasoning behind this transformation is the fact that any two categories can always be

separated by a hyper plane if transformed into a high enough dimensions space (Fukunaga 1990). Thus SVM machines can separate non-linear problem while still using the simple but elegant principle of linear machines.

There is a need to minimize the risk of over-fitting, which would result in bad generalization. The best generalization performance will be achieved if the right balance is struck between the accuracy attained on a particular training set and the ***capacity of the machine***, that is, the ability of the machine to learn any training set without error (Burges 1998).

A brief summary of the theory of support vector machines is given below (Cortes and Vapnik 1995).

Assume there is a set of training patterns

$(y_1,x_1)\ldots,(y_l, x_l)$ $\quad y_i \epsilon [-1, 1]$

These patterns are linearly separable (i.e. can be separated without error) if there exist a vector w and a scalar b such that

$$\mathbf{g}(\mathbf{w}.x_i + b \geq 1 \text{ if } y_i = 1, \qquad \textbf{Equation 2.5}$$

and

$$\mathbf{w}.xi + b \leq -1 \text{ if } y_i = -1, \qquad \textbf{Equation 2.6}$$

The above two equations can be written in a more compacted form as

$$y_i (\mathbf{w}.x_i + b) \geq 1 \quad i = 1,\ldots,l. \qquad \textbf{Equation 2.7}$$

The optimal hyper-plane separating such patterns with the maximal margin is

$$W_0.x + b = 0 \qquad \textbf{Equation 2.8}$$

If the training data is not separable then there with be some non-negative error

$\xi i \geq 0, \qquad i = 1,\ldots\ldots,l.$

The summation of such errors is

$$\Phi(\xi) = \sum_{1}^{i} \xi_i \qquad \textbf{Equation 2.9}$$

The goal will be to minimize the aggregate error subject to the constraints

$$y_{i\,(}\mathbf{w}.x_i + b) \geq 1 - \xi i\,, \qquad i = 1,\ldots,l. \qquad \textbf{Equation 2.10}$$

$$\xi i \geq 0, \qquad i = 1,\ldots\ldots,l. \qquad \textbf{Equation 2.11}$$

The patterns causing errors are the support vectors. If these patterns are removed from the training data , then it would be possible to separate the remaining patterns without errors by creating an optimal separating hyper-plane (Cortes and Vapnik 1995).

Such an optimal hyper-plane is created by minimizing the function;

$$0.5w^2 + CF\,(\sum_{1}^{i} \xi_i\,) \qquad \textbf{Equation 2.12}$$

Subject to equation 7 & 8

F (u) is a monotonic convex function and C is a constant.

The above hyper-plane is in the input space. However it is more convenient to create a hyper-plane in the features space. This is done by using a kernel function as the monotonic convex function above. The kernel function is convoluted with the input vector to move to the features space.

The four popular kernels functions used by SVM classifiers were considered. These are the linear, polynomial, radial basis function and the sigmoid kernel functions. The radial basis function was chosen as the most appropriate function to use in this study. This is because it can handle both linear and non linear vectors and has a superset of most

of the characteristics found in the other three kernel functions named above (Hsu et al. 2003).

Thus F (u) in the above equation can be replaced by radial basis function for this dissertation.

$$F(u) = \Phi(x_i) = \exp(-\gamma \|x_i - x_j\|2) \qquad \textbf{Equation 2.13}$$

Where γ = radial basis kernel parameter

The minimization problem can be restated in the features space as

Minimize

$$0.5w^2 + CF\left(\sum_{1}^{i} \xi_i\right) \qquad \textbf{Equation 2.14}$$

Subject to

$$y_i (w.\Phi(x_i) + b) \geq 1 - \xi i, \qquad i = 1,\ldots\ldots,l. \qquad \textbf{Equation 2.15}$$

and

$$\xi i \geq 0, \qquad i = 1,\ldots\ldots,l. \qquad \textbf{Equation 2.16}$$

Thus SVM machines find the optimal hyper-plane from the given training data by working out the above programming problem.

The SVM machines approach to building classification algorithms has had wide success and is one of the standard techniques now in use and typically taught in all graduate classes in pattern recognition. Thus, this method was eventually selected for the classification algorithm implemented in this dissertation. The next section discusses research on typing behavior since it is essential to understand what types of typing

variability can be expected from users of a keypad biometric because high individual variance will render such a method unviable.

2.10 Cognitive Aspects of Skilled Typing

A feasibility analysis of a proposed technological innovation needs to consider how the innovation will be used. In the case of the biometric keypad, a significant issue is the continued ability to classify users as unique despite normal changes in their data entry behavior. This section will discuss what is known about human typing patterns and how they behave over time, with different typing skills and with different distributions of keys. These variations are important parameters to consider since it is possible that they will affect the classification and therefore have to be accounted for in the development of the keypad biometric.

2.10.1 The Impact of Continued Learning on Classification

The first element that requires investigation is learning. As users continue to type a password or a PIN over time, they exhibit learning, that is, the time to key in the identifying token decreases until the person reaches some plateau level. In the next few paragraphs, this learning is discussed in relationship to a key issue with this learning, that is, does this learning change the unique keying pattern that identifies a person over time. If it does, then using the keying pattern as a classifier will not readily work especially when a user goes on vacation and does not use the key pattern for awhile.

Early work in psychology looked at the learning patterns that occurred in learning Morse code (Bryan and Harter 1899). The time to perform the perceptual skill of identifying patterns of dots and dashes was measured over time along with the time to

type in a sequence of code. The time to perform these skilled tasks was found to decrease steadily until it leveled off at some plateau. After a rest period, performance time was again found to start decreasing steadily until a plateau was again reached. This pattern continued to re-occur. Later studies confirmed the progressive learning curve and the plateau (Crossman 1959). Seibel (1963) trained three subjects in using a ten-finger keyboard and collected performance time for three months or for a total of 75,000 entries. He found irregularities in performance that occurred in a systematic manner. A run of trials closely spaced depressed the results, which recovered during an extended rest period. The results from this study and a large number of other studies on skilled motor performance indicate that performance improves over long periods of time and that the rate of improvement is reduced as practice continues. The results also indicate that irregularities occur in the learning curve depending on time between practice intervals, motivation and feedback on performance.

A user with a PIN number will type it numerous times. During each typing, learning will occur and the PIN number will be typed faster. However, it is not known whether the unique typing pattern captured in earlier learning and used to authenticate an individual will continue to remain reliable. There is some suggestion in the literature that it will not. In a study of inter-keystroke intervals (time between the completion of one keystroke and the start of the next), the inter-keystroke interval distributions were plotted for a subject learning to type at four weeks and at eight weeks (Gentner 1982). This was compared to two plots of inter-keystroke intervals for expert typists. It was found that the faster the typist, the more consistent the inter-keystroke interval was with that of the learning typist showing the largest change as typing skills progressed. These results

suggest that developing classifiers at an early stage in the learning of a PIN number may lead to poor classifier performance at a later time because the inter-key times will change in a nonlinear fashion. Studies on learning also indicate that mass practice is not a good method for capturing data for classification since mass practice will depress performance. Since typing with a keyboard is very different from learning to key in a small subset of characters, the impact of learning on classification errors needs to be explored more. An experiment described and analyzed in Chapters 5 and 6 will address the learning impact further.

2.10.2 Impact of Typing Skill on Classification

Researchers have for a long time been interested in characterizing individual differences in typing. In particular, they have conducted research to determine the characteristics that differentiate a skilled touch typist from a novice typist. This research is of importance to this dissertation because these differences may affect the ability to develop unique classifiers for specific types of typists. For example, skilled typists, as shown in the above described study by Gentner (1982) have consistent inter-key times making it difficult to find the variances for this parameter that aid discrimination. Novice typists generate so much noise in their inter-key times that this variance would also make it hard to build classifiers. The paragraphs which follow describe additional research that investigates differences in typing skills which may impact classification.

Long et al. (1982) analyzed differences and similarities between sixteen female typists. The subjects were asked to type standard English prose of approximately 2000 characters. The instruction for each typist was to type as fast as possible without making

more than 1% errors. Measurements of the inter-key time were recorded. The distribution for the inter-key times was plotted for each of the subjects showing large individual differences among them. An analysis of these distributions showed that highly skilled typists exhibited significantly larger skewness and kurtosis in these distributions than less skilled typists. Nevertheless, each typist, whatever her typing speed, exhibited a unique inter-key time distribution suggesting that classification rates should go up for skilled typists. It is not known how keying time or pressure vary with typing skill, but it is postulated that they will vary in the same way as inter-key times, i.e., be more consistent for skilled typists. Thus, any study of other parameters that might affect classification rates needs to take into account typing skill. This is done in the experiment described in Chapters 5 and 6.

2.10.3 Impact of Different PIN Patterns on Classification

Another key issue with classification is the impact of the pattern of keys typed on the ability to classify, e.g., the pattern "4321" might be easier to classify than the pattern "1234." Studies conducted on typists suggest that this might be so. In a study by Gentner (1982), it was found that inter-key time for one digraph was found to have more variability than another digraph. For example, he found that the distribution of inter-key times for the digraph "ce" had a median of 204 msec and a half-width of 20 msec, but the "ne" distribution had a median of 120 msec and a half-width of 41 msec. Thus, some key combinations, because of their higher variance may be harder to classify than others.

Another study showed that in a number of cases the inter-key interval for a given digraph differed significantly depending on the word in which the digraph was embedded

(Terzuolo and Viviani 1980). For example, they found that the inter-key interval for the digraph "an" was 147 msec in the word "thank" and 94 msec in the word "ran." A simulation model was for typing in which keystroke timing was based on keyboard layout and the physical constraints to the hands (Norman and Rumelhart 1982). They found context effects similar to those found by Shaffer (1978) which were explained by key distances and hand interchanges in the keying pattern. It is likely that longer inter-key typing patterns are more likely to exhibit differences among users and be easier to classify. However, no studies have been made on the individual differences found between these digraphs nor on the relationship between PIN patterns and classification. It is also likely that differences in PIN patterns are affected by differences in typing skills. This is explored further in the experiment described in Chapters 5 and 6.

2.11 Acceptance of Biometric Keyboards

Keyboard-based authentication is an evolving technology that proposes to modify the way users gets authenticated. Such a new technology can either be accepted or rejected by the users. Acceptance of such a technology would lead to the proposed advances in authentication while rejection would lead to wasted resources in terms of money and effort invested. Thus understanding and anticipating issues that would lead to acceptance or rejection of such a technology early in the development process is very important. The first part of this section presents the process and the results of stakeholder's identification. Although many stakeholders are involved in any technology development, two groups of stakeholders were identified as relevant to the research in this dissertation. These are the organization managers who make the decision to adopt a new product and

the end-users who make the decision to use a product that is provided for them. The manager is relevant because this person makes the purchase decision for the adoption of a keypad biometric. To assess the potential viability of a keypad biometric, the factors that influence this adoption decision need to be known. The end user is also relevant because this person makes a choice to use or not use a keypad biometric. Thus, the factors that affect the end user's acceptance need to be known. Most of the adoption and acceptance factors have been identified in prior research but not necessarily combined to match the adoption (by managers) and acceptance (by end-users) of a biometric innovation. The next sections identify these factors that will be combined in Chapters 7, 8, 9 and 10.

2.12 Important Factors for Successful Adoption of Biometric Keypad

Organizational managers are charged with the responsibility of determining what product to adopt. In so doing, they have to consider several issues. Rogers (1995) gives the important components of the adoption process as the innovation, communication system, time, and the social system as shown in the figure below.

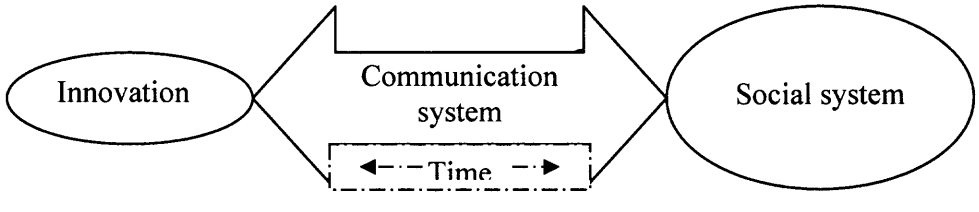

Figure 2.3 Elements of adoption process –Adapted from Roger (1995)

Each of these components has its own set of issues that can affect the adoption process. The innovation in our case will be the new keyboard-based authentication technology. Rogers (1995) suggests that important questions that researchers need to

address are the perceived attributes of an innovation and their effect on the rate of adoption. In the case of the keypad biometric, the perceived attributes are not only those perceived by the manager, e.g., reliability and ease of maintenance, but also those that the manager believes customers will perceive as important, e.g., ease of use or invasion of privacy.

The next issue that affects managerial adoption is the media through which the innovation idea is transmitted from the producer of the innovation to the manager. The efficiency and effectiveness of the communication channels will determine the number of new users that get to hear of the new innovation and the rate at which these messages get passed on. In addition managerial adoption is affected by the social system that they are embedded in. Rogers (1995) defines the social system as a *set of interrelated units that are engaged in joint problem –solving to accomplish a common goal.* In this research, it is the organization that will be adopting the new keyboard based technologies.

Adoption is typically measured as the rate at which it occurs. Thus, time is a key element especially in terms of indicating the rate of technology adoption in an organization. The figure below lists the key factors that have been found to affect the rate of adoption of a new technology.

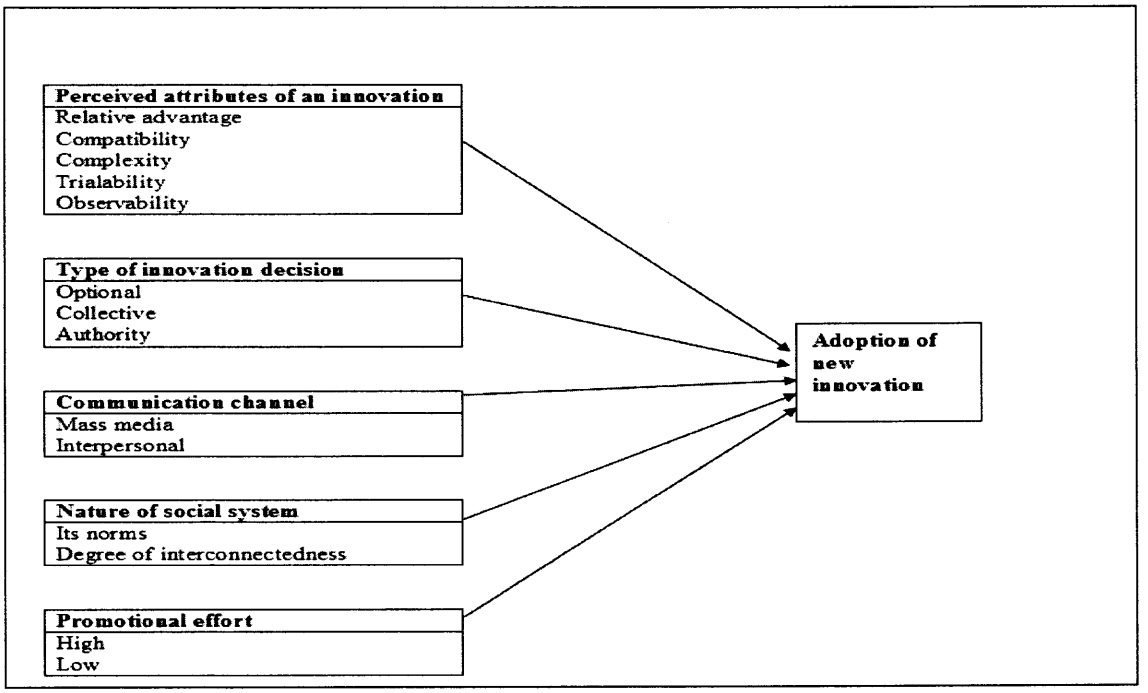

Figure 2.4 Variables determining the rate of adoption of innovations (Rogers, 1995)

The research in this dissertation will focus on the perceived attributes of the innovation and their impact on adoption. Although the others are clearly viable, this work is primarily concerned with developing a keypad biometric, and, as such, is focused on the properties that are embedded in this technology, either real or virtual, that will impact its feasibility and final use.

2.13 Important Factors to Successful User Acceptance

In contrast to adoption, end users of many technologies are not making a conscious decision to adopt the technology so much as a decision to use the technology once it has been provided for them. For example, escalators have been installed in many buildings. With their installation, end users, e.g., shoppers in a department store, could easily avoid

using the escalators by walking up and down stairs, and certainly, some users have chosen to do so, but most have chosen to accept the innovation, so much so, that management must now continue to install and maintain escalators because they are considered a standard technology found in public places. Other technologies that have been adopted by management but not been accepted are touch screen information kiosks at airports and in hotels.

The acceptance of the biometric keypad by the end user is the final determinant of the success of the biometric keypad and something a manager must consider in the decision to adopt the technology. There are several models from the literature that attempt to explain the factors that would be important to the end user in determining whether to accept or reject a new innovation. The next subsections reviews three of the most popular models, which are the technology acceptance model, web of systems performance model and the unified theory of acceptance and use of technologies model.

2.13.1 Technology Acceptance Model-TAM

This is probably the most popular model in the technology acceptance literature. The model indicates that the behavioral intention to use a new technology depends on its perceived usefulness and its perceived ease of use (Venkatesh 2000).

TAM has proved to be simple and powerful in explaining the behavioral intention to use various information technologies (Venkatesh 2000). However it is at a very high level and therefore difficult for designers to operationalize at the implementation level (Venkatesh et al. 2003).

This is shown graphically in the figure below.

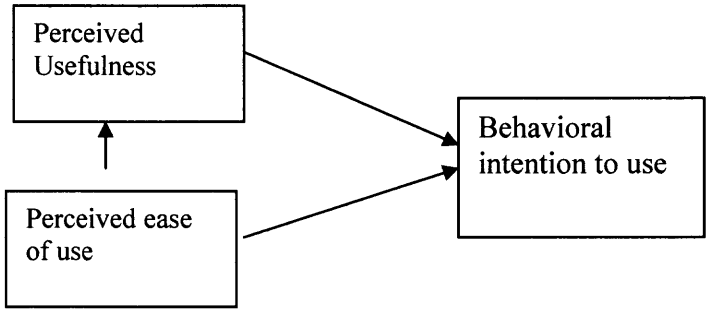

Figure 2.5 Technology Adoption Model

Several extensions have been suggested to the TAM model among the most notable being the addition of the "trust" construct (Gefen et al. 2003). This trust construct is likely to be very relevant in the introduction of the keyboard biometric authentication technology.

2.13.2 The Web of System Performance-WOSP Model

Another recent model explaining the acceptance of technology (with a focus on security) is the WOSP model. This model borrows from systems theory and extends TAM by including other constructs which emphasize performance and security issues (Whitworth and Zaic 2003). The WOSP model consists of four factors likely to enhance acceptance. They are good functionality, flexibility, extendibility and connectivity. The model also lists four factors that are likely to damage acceptance. They are poor usability, security, reliability and confidentiality.

The WOSP model posits that pairs of the above named constructs acts in tension such that an increase in one may result in a decrease in the other. For example, adding functionality may make the interface to a technology more complex and thus, make it less

usable. As shown in the diagram below, functionality is in tension with usability, extensibility is in tension with security, reliability is in tension with flexibility and connectivity is in tension with confidentiality. An increase in one of the factors in tension puts tension on its member and, to a lesser extent, to the other members of the web although it is also possible to extend the web by pulling on two opposing member factors, i.e., by increasing the quality of both factors.

The WOSP model is closer to explaining most of the constructs found in the biometric literature making it a likely candidate to use for selecting the factors to investigate in determining the acceptance feasibility of a keypad biometric. However, the WOSP model is a rather new model and needs more validation and testing over time to examine its predictive power for the acceptance of new technologies.

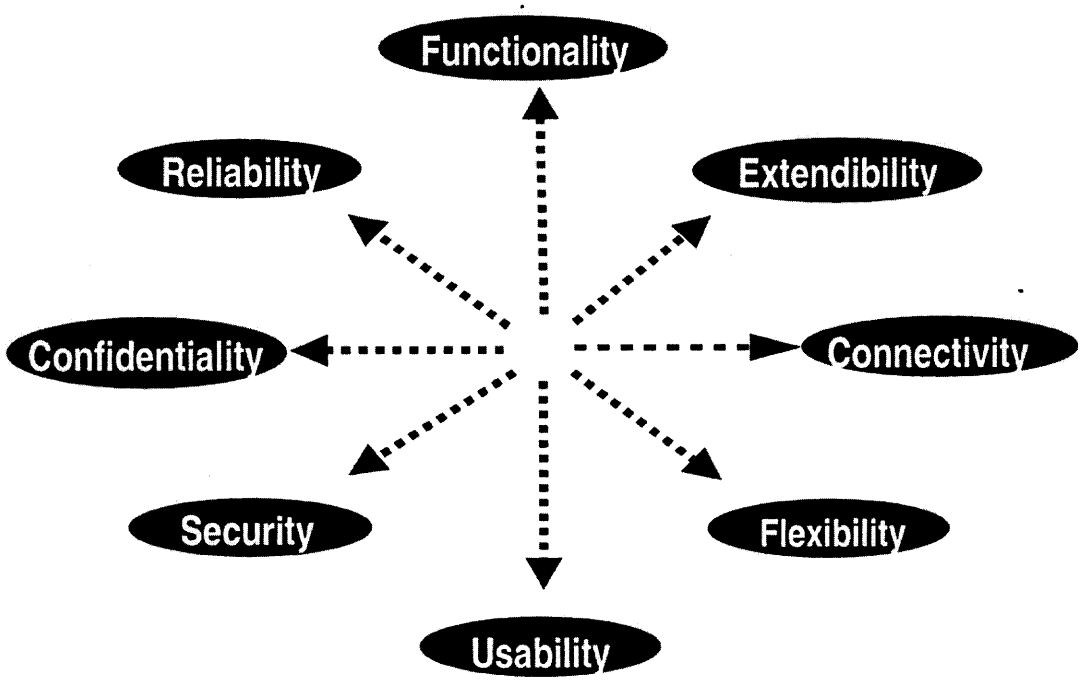

Figure 2.6 WOSP Model (Whitworth and Zaic 2003)

2.13.3 Unified Theory of Acceptance and Use of Technology-UTAUT

The UTAUT model is an integration of eight of the leading technology acceptance models (Venkatesh et al. 2003). It proposes that the behavioral intention to use a new technology depends on four major theoretical constructs namely, performance expectancy, effort expectancy, social influence and facilitating conditions. These constructs are defined as follows (Venkatesh et al. 2003).

Performance expectancy *is the degree to which an individual believes that using the system will help attain gains in job performance.* This includes some of the previously studied constructs of perceived usefulness, extrinsic motivation, job fit, and relative advantage and outcome expectations. In the case of the keypad biometric, this translates into the degree to which the end user will perceive that its use will protect him or her from identity fraud.

Effort expectancy is the *degree of ease associated with the use of the system.* Ease of use was found to be very important especially in the early stages of an innovation introduction. The construct includes perceived ease of use and complexity. In the case of the keyboard biometric authentication system, this translates into how much effort the end user thinks the training will be and how much of a problem using the system will be if the PIN has to be retyped a number of times.

Social influence is the *degree to which an individual perceives that important other believe (s)he should use the new system.* Related sub-constructs include social norm, image and social factors. For keypad biometrics, social influence could translate into work influences that encourage the use of a biometric keypad for security-related reasons.

Facilitating conditions *is the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system.* Sub-constructs included are behavioral control and compatibility. For the keyboard authentication system, this could translate into additional mechanisms that support alternate authentication when keyboard authentication fails.

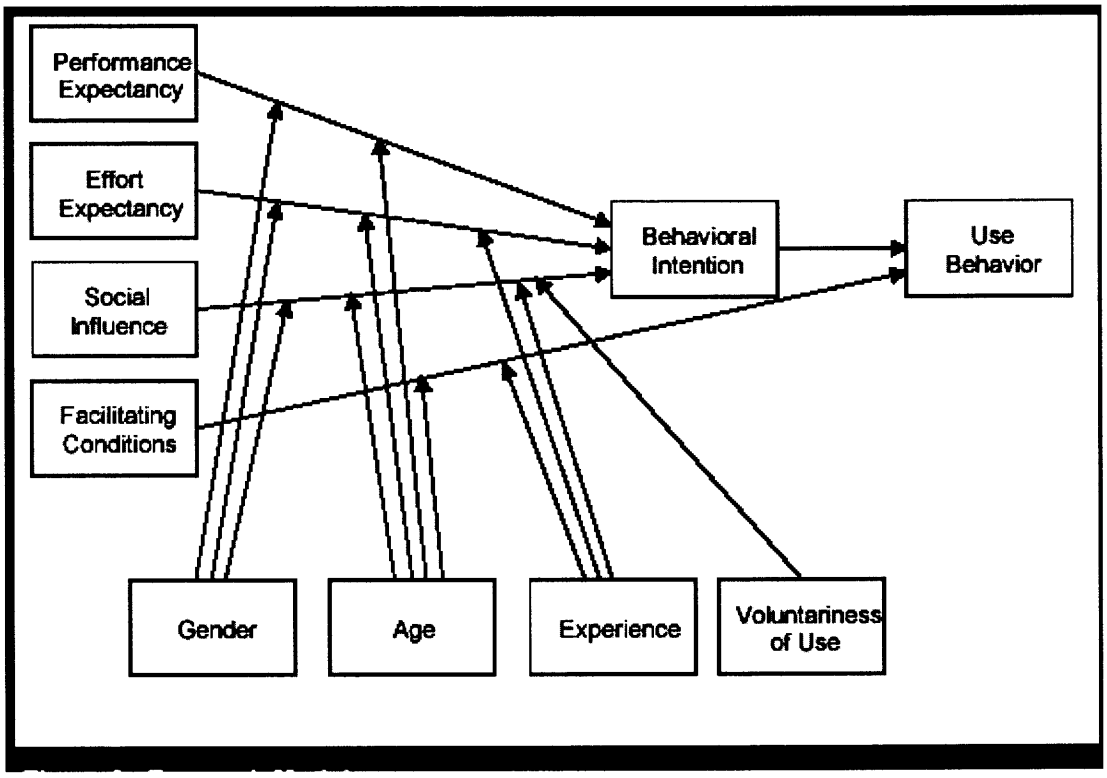

Figure 2.7 Unified model (Venkatesh et al. 2003)

The above model was shown to explain a significant amount of the change in the behavioral intention to use variable (R^2= 0.69). This is the highest performing model compared to the other models considered. It will be revisited in the sections of model

building and the definitions given above will be used in this dissertation with some extensions.

2.13.4 Gaps in Technology Acceptance Literature

Getting new technologies adopted or accepted is a difficult task even when they have outright advantages over the existing technologies (Rogers 1995). This makes it important to understand the critical factors necessary for successful acceptance of new technologies like the biometric keyboards. A search was done using previous work in technology acceptance and in evaluation of biometric technologies for a model that could be used to predict acceptance of a new biometric technology. For the three models discussed above, it was not possible to apply the critical factors researched without some adaptation to specific key-pad biometric issues. The first problem was that the technologies studied in validating the previous models were simple technologies that provided workplace functionality for users at a cost of learning to use the system (Venkatesh et al. 2003). None of the models had been tested with biometric technologies, which are more complicated and have a large number of social issues that could affect acceptance. The second problem was a difference in the type of user being targeted. The acceptance models reviewed above were all formulated by members of the Information Systems community who have backgrounds in IS theories and constructs. Designers of biometric technologies have no experience with information systems theoretical constructs. There is, therefore, a need to translate and granularize high level constructs used in technology acceptance models to every day concepts that biometric designers are familiar with. The third problem is a mismatch between the factors that are

deemed important in the biometrics field compared to those appearing in the IS models. A comparison of the models to the biometric literature reviewed earlier in the evaluation of biometrics section shows that there are several important factors in the biometric literature that do not appear or are not given enough attention in the information systems models. These factors include systems intrusiveness, systems vulnerability to external attacks, false acceptance and false rejection rates and perceived security advantage.

Due to the above problems and mismatches, a decision was made to extend the state of the art by building and validating a prediction model for biometrics. The second and third studies of this dissertation will give details on how this was achieved and the contribution that this is expected to make in both the IS and the biometric technologies communities.

2.14 Summary

This chapter reviewed the current authentication technologies and identified one of their key shortcomings as the use of external identifiers. An addition of a biometric layer was suggested as a solution to the problem. Different types of biometrics were presented and the criteria used to evaluate them given. These biometric technologies were then compared and the biometric keyboard chosen as a biometric technology with the potential of providing a second layer to the existing authentication systems. Previous work on biometric keyboards was reviewed and several gaps identified which will be addressed by this research. The process of developing the biometric keyboard was overviewed and support for the choice of classification features, wavelet analysis and choice of classifiers given for the pattern recognition and classification task.

Different cognitive aspects of skilled typing which may affect the performance of the biometric keyboard were then considered. Lastly, various factors that could be important in the adoption and user acceptance of the biometric keyboard were extracted from the literature and discussed. The next chapter presents the research questions covered in this dissertation and the process this dissertation will take in investigating these questions. The questions and especially the process are developed from the literature just reviewed in this chapter.

CHAPTER 3

RESEARCH QUESTIONS

3.1 Introduction

The previous two chapters gave the background to the research problem addressed in this dissertation and the previous work conducted in the design and acceptance of biometric keyboards. This chapter presents the research questions that guided this dissertation and an overview of the research procedures that were used to answer the research questions.

3.2 RQ 1: Technical Feasibility of Biometric Keyboard

Chapter 2 showed that the growth of the information-driven society has revolutionized the way financial transactions are undertaken. Most of these transactions are now conducted remotely from the home or office. The mode of payments has changed from cash to plastic and electronic transfer. This provides easy access to remote financial resources from any place at any time.

The flip side of this progress is a proliferation of personal information databases. This proliferation has increased the data vulnerability points and the uncertainty of the identity of the remote party. It has become more difficult to say with certainty that the person on the remote side is really the person that he/she is really claiming to be. This has led to increased cases of identity fraud, which if left unchecked, will become a major impediment to the national growth and a threat to e-business. The need for solutions that can mitigate the problem has never been greater.

A closer look at transactions shows that there are common patterns in most identity fraud cases. One of the common threads in all transactions is that users have to go through a keypad in order to reach the financial systems, systems of records or e-commerce systems. In cases where the user is dealing with a physical attendant, for example in the bank, or in the supermarket store, the user still has to use a keypad for identification and verification purposes. Likewise an identity thief must go through the keypad before accessing the victim's accounts. A hacker, intent on stealing other people's personal information must also go through the keypad. Thus the keypad seems to be an attractive gate keeping point from which authentication can be performed. This leads to the first research question.

RQ1: What is the technical feasibility of performing authentication at the keyboard gateway?

3.3 Procedures for Answering RQ 1

The above research question is answered in three stages. The first stage investigates the technical feasibility of authentication at the keying point of entry. The second stage examines how well the proposed authentication method will perform in real life. The third stage gathers user data on how they intend to interact with the technology. This user data feeds back into the first stage by defining the boundaries of the classifier data collection and reliability requirements.

It was pointed out in Chapter 2 that using external identifiers from user methods such as a personal password or a token could readily be duplicated by an imposter and that a measure that was unique to the biology of the user would be more reliable. A

number of biometric methods that have been tried for such authentication such as fingerprint recognition, iris scanning, voice recognition, etc. were reviewed, and it was ascertained that these methods were either expensive, intrusive or inappropriate. Literature on classification by keying patterns was covered and shown to be reliable in a laboratory setting. Thus, a keyboard biometric is suggested as a potential mechanism to explore with this dissertation. However, there were several questions concerning the technical feasibility of the keyboard biometric that have not yet been completely researched by others. First, most of the research has been done on keyboards with either a large amount of text being used to recognize individuals. Thus, the first research sub-question to be asked is: (1) Are individual typing patterns unique for a numeric keypad using a small (4-6 digit) number for authentication? Prior research on keying biometrics has used time latencies, e.g., inter-key times, key-down times, and key diagraphs. Because each individual research did not compare results using a consistent standard, it was unclear which collection of parameters would be optimal for classification. Chapter 2 compared the results and found that key down time and inter-key times achieved the best classification results. Thus, these values were used to address the second technical feasibility research sub-question: (2) What are the optimal characteristics of the input signals that should be used for classification of different users?

The development of keyboard classification algorithms was also found to use a variety of methods for mathematically modeling the typing patterns of users. These included Fourier transforms, wavelet analysis and geometric waveform analysis. Wavelet analysis was shown to be superior to the other methods, in particular because it retains both frequency and time position information. Thus this research will use wavelet

analysis to model the keying data which provides an answer to the next research sub-question: (3) what method is best for characterizing the pattern differences produced by individual typists?

Prior work on keypad biometrics used neural networks learning, linear classifiers, Bayesian classifiers and quadratic classifiers to achieve their approximately 90 percent accuracy rates. There are a wide variety of techniques available and newer techniques have been developed since some of the keypad biometric development work has transpired. Each of the classification techniques has different advantages, e.g., the amount of time it takes to train the classifier or whether the classifier is good at working on non-linear patterns, etc. Thus, a part of this research will investigate the following research sub-question: (4) which are the most appropriate classifiers for biometric keypads?

Although not investigated, two studies discussed in Chapter 2 suggested that the addition of pressure would be likely to improve classification. This is not unexpected since using another dimension typically improves classification, but using pressure implies the development of a keypad that captures this dimension. Thus, two final research sub-questions are addressed in this section of the dissertation. (5) How should a pressure keypad be built and sampled to provide pressure data to the classifier engine? and (6) Would the addition of pressure pattern features to the time pattern features improve discrimination accuracy? This second question will be addressed following the execution of stage two which collects a set of data to examine other technical feasibility questions posed in this dissertation. A simulation will be run on this set of data that will classify subjects both with the use of the pressure parameter and without this usage. The

classification rates will then be compared to determine if pressure improved classification.

Having laid out the process for establishing the technical feasibility of the keypad biometric in stage one, the next stage involves evaluation of the performance of the biometric keypad under various field conditions that would characterize the use of the biometric keypads. First, variations in human behavior are considered. The prior research on typing behavior covered in Chapter 2 indicated that people who are novice typists have more erratic typing patterns than people who are expert typists. This suggests that it will be easier to classify users who are good typists leading to the following research sub-question: (7) How much will variations in typing speed impact classification performance? Research presented in Chapter 2 also indicated that typing performance degraded if time elapsed between typing episodes. The studies measured errors and typing speed but not the individual characteristics of the typing. This prior work suggests that elapsed time between keypad entries might affect the time and pressure characteristics of a keying pattern. However, it is possible that the pattern will linearly degrade so that the classification will not be impacted, but this is not known. This leads to the following research sub-question: (8) what is the effect of elapsed time on the classification performance?

Typing studies have also shown that patterns for typing different words are distinctly different. This is true, in part, because the distance a finger has to travel to find a key affects the inter-key times, but it also true because some patterned sequences are overlearned, i.e., typing "the" is very fast because of the large amount of practice this sequence of characters has had. The research described in Chapter 2 also found that the

surrounding letter context affected a typing pattern, i.e., if "the" was embedded in another word such as "wither," its typing pattern would differ from that of being embedded in the word "these." Although it is not known whether this might be true, prior work suggests that different personal identification numbers may be harder to classify than others leading to the research sub-question: (9) Are there differences in classification performance for different pin numbers?

Other human behavior possibilities for variations in classification performance that this dissertation does not address include (1) the impact of stress on typing patterns, (2) the impact of fatigue on typing patterns, (3) the impact of illness on typing patterns, etc.

Second, the environment may have an impact on the ability to effectively classify patterns. For example, users may type differently in different weather conditions or in different levels of public exposure, e.g., at an ATM on a busy street. These effects are also not addressed in this dissertation.

A third area of possible impact is variability in the system that is measuring the typing patterns. For example, the pressure sensors may become loosened over time and give lower values than before. External elements may become embedded in the keypad causing higher readings, e.g., gum or sneezed-on orange soda. This dissertation does not investigate these impacts on the technical feasibility of the keypad biometric.

The third stage of this research addressing technical feasibility issues relates directly to the first stage which develops the biometric classifier. The original development made assumptions about the availability of learning data. This assumptions need to be tested since they relate to how willing the end user is to generate multiple

patterns. These lead to the following research sub-question: (10) How many training iterations is a typical user willing to engage in to generate data to develop their personal biometric keypad classifier? There is also an implied assumption on what is an acceptable False Rejection Rate leading to the following research sub-question: (11) what is an acceptable false rejection rate under various user circumstances? These questions will be posed in the survey that is distributed in the research being performed to answer Research Question 2 in this dissertation.

3.4 RQ 2: Acceptance of Biometric Keyboard Technology

Biometric methods may offer certain advantages over traditional authentications methods. However, the uptake of biometric technologies has been lower than earlier forecasted (Albrecht et al. 2003). This may be because certain issues need to be addressed before a critical mass of potential users become comfortable with the use of biometrics. Thus, *proof of concept* that a keyboard-based authentication system can be built (RQ1-technical feasibility) does not necessary imply that such a technology would be accepted if built. There are many technically feasible products which failed to succeed in the market due to failure to address acceptance issues. Chapter 2 discussed acceptance issues and presented the innovation development process proposed by Rogers (1995). This is shown in the figure below. This product development process is a long and costly process in terms of capital and manpower investment. To minimize the risk of failure, there is need to look ahead and identify the critical technology factors that must be satisfied for such a prototype to be accepted by the users. Research Question 1 addressed the first three stages of this process. This dissertation is focused on the

feasibility of an innovation and so will also address the next to last stage of the process, "Diffusion & Adoption" for its second research question.

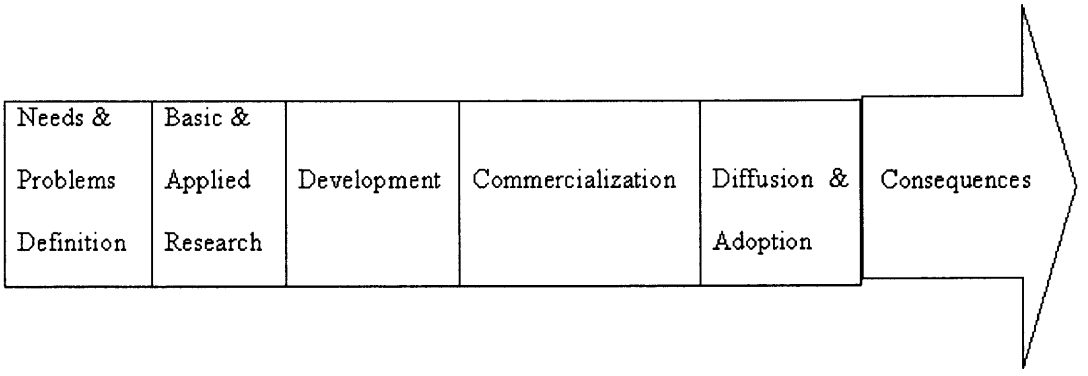

Figure 3.1 Innovation development process (Rogers 1995)

RQ2: *What are the critical factors that would determine the acceptance of a new biometric technology similar to the key-based authentication product?*

3.5 Procedures for Answering Research Question 2

The first step in answering the second research question was an analysis of the needs of the key stakeholders in the product development process. There are two key groups of stakeholders in the product development process that impact adoption. They are: the management of potential organizations that might be purchasing the biometric keypad and the end users of the keypad biometric that decides whether they will use such a keypad if it becomes available to them.

A key part in examining whether an innovation will be adopted is in determining what critical factors affect adoption. Both knowing these critical factors and stakeholders responses to them will help to assess whether a keypad-based biometric is likely to be adopted. The critical factors that have been found to affect adoption and acceptance were

discussed in Chapter 2. (Note: *Adoption* refers to a decision to actively take all the steps necessary to acquire, install, and use a new technology, Acceptance assumes that a new technology is in place and refers only to a decision by each individual user to actively use the technology.) Two studies are conducted to measure what critical factors exist and the stakeholder's responses to these critical factors. The first study is conducted on the decision makers who are likely to make purchase decisions for a keypad biometric technology installation. The adoption literature mentions potential critical factors that might be important, but a keypad biometric might bring out additional issues that were not addressed in this literature. In particular, it is desired to know what critical factors these people might think would affect their customer's acceptance of the biometric technology. This is important because a critical factor for acceptance will affect the decision by an executive to adopt the technology. Thus, although multiple adoption critical factors are known, what additional customer acceptance factors might exist for this relatively sensitive technology are not known. Thus, the study with executives addresses the following research sub-question: (12) what critical acceptance factors do executives believe will impact end user acceptance of a keypad biometric? In addition, the literature reviewed on adoption lists the factors affecting adoption but does not indicate what their relative importance might be especially for biometrics. This leads the first study to examine the following research sub-question: (13) to what extent wills the critical adoption factors presented in the research literature impact adoption for a keypad biometric? Finally, it may be that the keypad biometric involves new issues that are relatively minor in other types of adoption. In particular, a biometric technology is more invasive than other types of innovations, not only changing the weights of importance for

the critical adoption, but also adding new factors. This leads to the following research sub-question: (14) What, if any, new factors will affect executive adoption of the keypad biometric?

The issues that are important to end user acceptance were addressed in a study that drew its critical factors from the literature covered in Chapter 2 and from the study conducted on the executives. The literature review drew critical factors from two sources, (1) the Unified Theory of Acceptance and Usage of Technologies (UTAUT) (Ventakesh et al, 2002) and (2) the biometric literature. In particular, the critical factors selected from the UTAUT model were adapted to fit the methods of presentation in the biometric literature. For example, ease of use included measures on how happy a user would be if he or she were rejected by the system a number of times. Based on the UTAUT model with the extensions from the biometric literature, the following hypotheses were proposed for assessing user acceptance of the keypad biometric. The constructs in these hypotheses stem from the following research sub-question: (15) What factors will affect the acceptance of the biometric keypad by the end user?

H2a: There will be a positive correlation between behavioral intention to use and *Performance Expectancy*

H2b: There will be a positive correlation between behavioral intention to use and *Social Influence*

H2c: There will be a positive correlation between behavioral intention to use and *Facilitating Conditions*

H2d: There will be a negative correlation between behavioral intention to use and *Effort Expectancy*

An additional factor arose from the interviews with executives who believed that a key issue in acceptance of the keypad biometric would involve a user's trust of the organization using the biometric and a user's concern about invasion of personal privacy. Thus, a fifth hypothesis tested to address Research Question 2 was:

H2e: There will be a positive correlation between behavioral intention to use and *trust-privacy expectancy*.

The above hypotheses will be addressed in Chapter 8 which conducts a user survey and builds a structural model to assess the relationship between these critical factors and acceptance. Although the factors used in the UTAUT model have been examined before, they have not been adapted to assessing the impact of biometrics and the trust / privacy factor has not been widely used.

3.6 Summary

This chapter reiterated the need for solutions to mitigate identity fraud. Two research questions on the technical and business feasibility of using biometric keypads to mitigate identity fraud were proposed. The research approach taken to answering these questions was then laid out. It included (1) investigating the best pattern modeling and classifying techniques to use, (2) running user studies to assess "in the field" issues associated with a biometric keypad system, (3) conducting a study on executives to ascertain what factors they considered important in deciding to adopt a keypad biometric and (4) conducting a

study on end users to determine which factors were most important in their acceptance of a keypad biometric.

The next chapter addresses the first aspect of this work, the investigation of the patterns modeling and classification techniques.

CHAPTER 4

INVESTIGATION OF BIOMETRIC KEYPAD TECHNICAL FEASIBILITY

4.1 Introduction

The goal of this chapter was to investigate the technical feasibility of the biometric keypad. The chapter starts by giving the research questions that were to be investigated in this study. The chapter then gives an overview of the prototype that was built to provide a test-bed for this investigation as well as the evaluation of the keypad biometric under various field conditions as given in the next two chapters. This is followed by an overview of the subjects and procedures used for this stage, followed by the data analysis procedures. Finally, the results and implications of the study are given.

The theoretical background for this chapter was given in Chapter 3 while the research questions and the roadmap to be followed in investigating technical feasibility were given in Chapter 3, Section 3.3. The four research sub-questions to be investigated in this study as summarized below for ease of reference.

Table 4.1 Research Sub-Questions 1-4

No.	Research sub-questions
1	Are individual typing patterns unique for a numeric keypad using a small (4-6 digits) number for authentication?
2	What are the optimal characteristics of the input signals that should be used for classification of different users
3	What method is best for characterizing the pattern differences produced by individual typists?
4	How should a pressure keypad be built and sampled to provide pressure data to the classifier engine?

The next section gives an overview of the prototype architecture so that the reader can understand the procedures followed and the results obtained.

4.2 Prototype Architecture

The section starts by presenting an overview of the main modules of the prototype. The modules are then joined together to show the full systems architecture.

The biometric keypad prototype is made up of several modules, each with a specific function. The modules are; (1) custom keypad module, (2) feature extraction module, (3) database module, (4) data cleaning module, (5) wavelet transformation module; (6) optimal parameters search module, (7) classifiers module, and (8) decision module. The following subsections present the function of each module.

4.2.1 Custom Keypad module

This is the first component of the prototype as shown in the diagram. It is made up of a standard keyboard that has been fitted with pressure sensitive resistors below each of the number pad keys. The voltage across these resistors increases when pressure is applied to the key digits and vice-versa.

4.2.2 Feature Extractions Module

The feature extraction module is the second block in the diagram. It monitors and records the voltage across the pressure sensitive resistors for each of the keypad digits. The module then extracts the inter-key time, key-down time and the voltage values for each

pulse. The details of how this process work is given in the next section on prototype development.

4.2.3 Database Module

The database module stores two sets of tables for the biometric keypad data. The first set of tables contains the raw data streams of the pressure voltage that is monitored across each pressure sensitive resistors. There is a table for each key. The second set of consist of the actual voltage pulses after data cleaning.

4.2.4 Data Cleaning Module

The function of the data cleaning module is to separate the actual voltage pulses generated on pressing the PIN sequence from the raw data streams.

4.2.5 Wavelet Transformation Module

The wavelet transformation module calls the wavelet toolbox from Matlab™. The later process the voltage pulses to produce wavelet coefficients which are used for classification. The details for this will covered in the next section.

4.2.6 Module for Computing Best Classifier Parameters

The function of this module is to search for the optimal SVM classifier parameters that will be used in all the subsequent classifiers. There are two important parameters for the radial basis function (RBF) kernel based SVM classifier (C, γ) which determines the performance of any RBF classifier. More details are given in the subsection on development of SVM classifiers in this chapter.

4.2.7 The Classifiers Module

The classifier modules consist of three classifiers. The function of the classifiers is to build a model of the given training data and use this model to classify unknown patterns into their correct classes. The first classifier is trained on the time-based features, the second one on pressure-based features and the third one on combined time and pressure-based features. The classifiers are then tested to verify technical feasibility.

4.2.8 Decision Module

This module makes the final decision on the class label of any given pattern. The module was not fully developed for this dissertation but it should ideally make a vote based on the output of the three classifiers or use any other accepted method of fusing multiple classifiers outputs. This will be done in a future study.

4.2.9 Block Diagram of the Prototype Architecture

The above subsections examined the different modules that made up the biometric keypad architecture. The diagram below combines all the explained modules so that the reader can get the full picture.

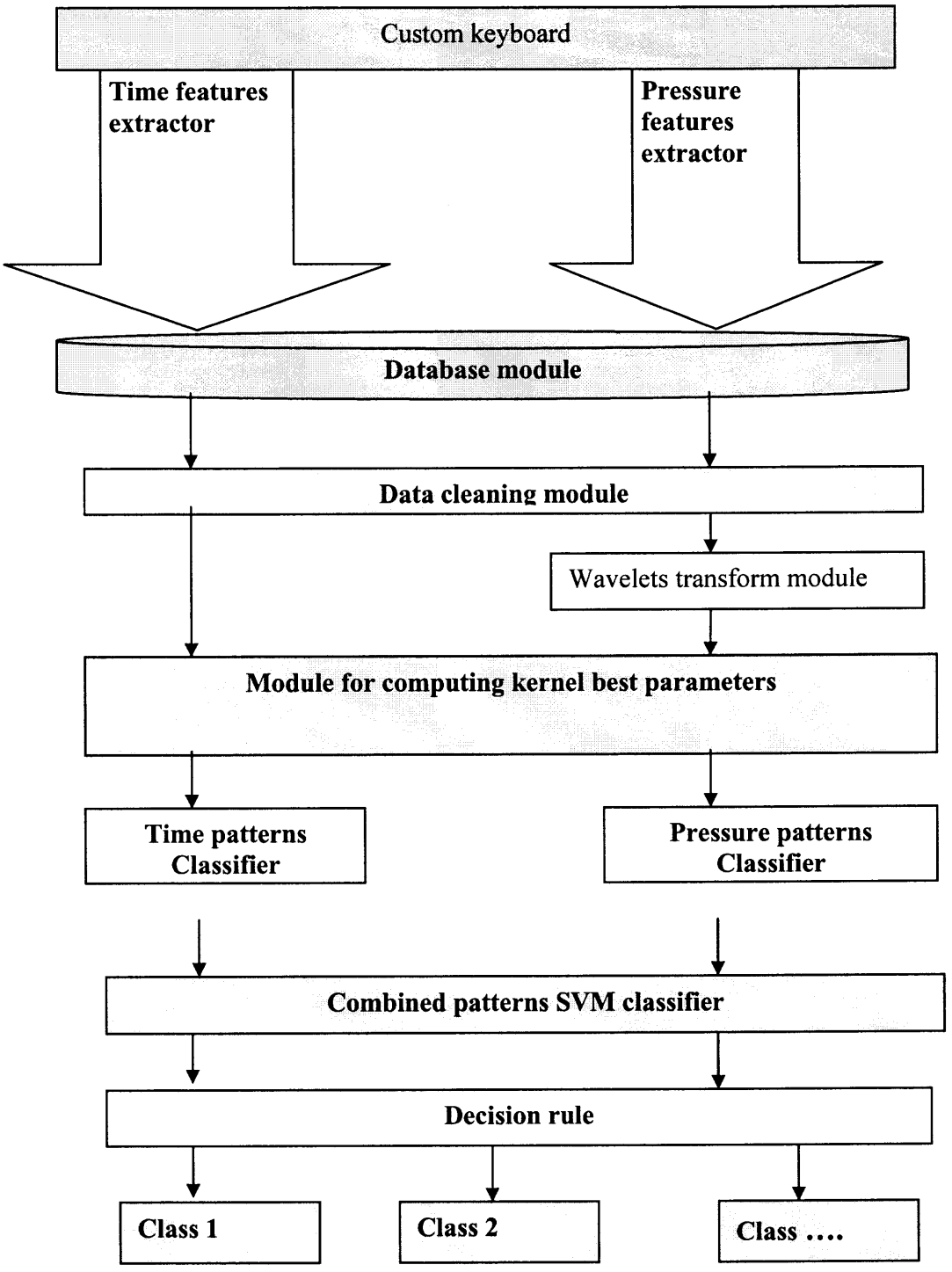

Figure 4.1 Architecture of the biometric prototype
The biometric prototype is made up of several modules. The functions of each module are explained in the preceding section.

4.3 Subjects

The above section presented and explained the working of the biometric keypad prototype. The development of the biometric prototype required data for training and testing the prototype to demonstrate its technical feasibility.

Four PhD students in a university in the east coast were used as subjects when developing the prototype. Two of the subjects were male while the other two were female. The ages were between 30 and 40 years old.

4.4 Experimental Procedures

The procedures developed during this section were later extended and refined as reported in the next chapter on research design of the main factorial design experiment. The subjects were first introduced and trained on the experimental task. The task consisted of answering world trivia questions followed by typing of the allocated personal identification number. The subjects were given time to practice answering the questions until they felt confident and their patterns were stable. The interface for the world trivia question is shown below to help the reader visualize the task.

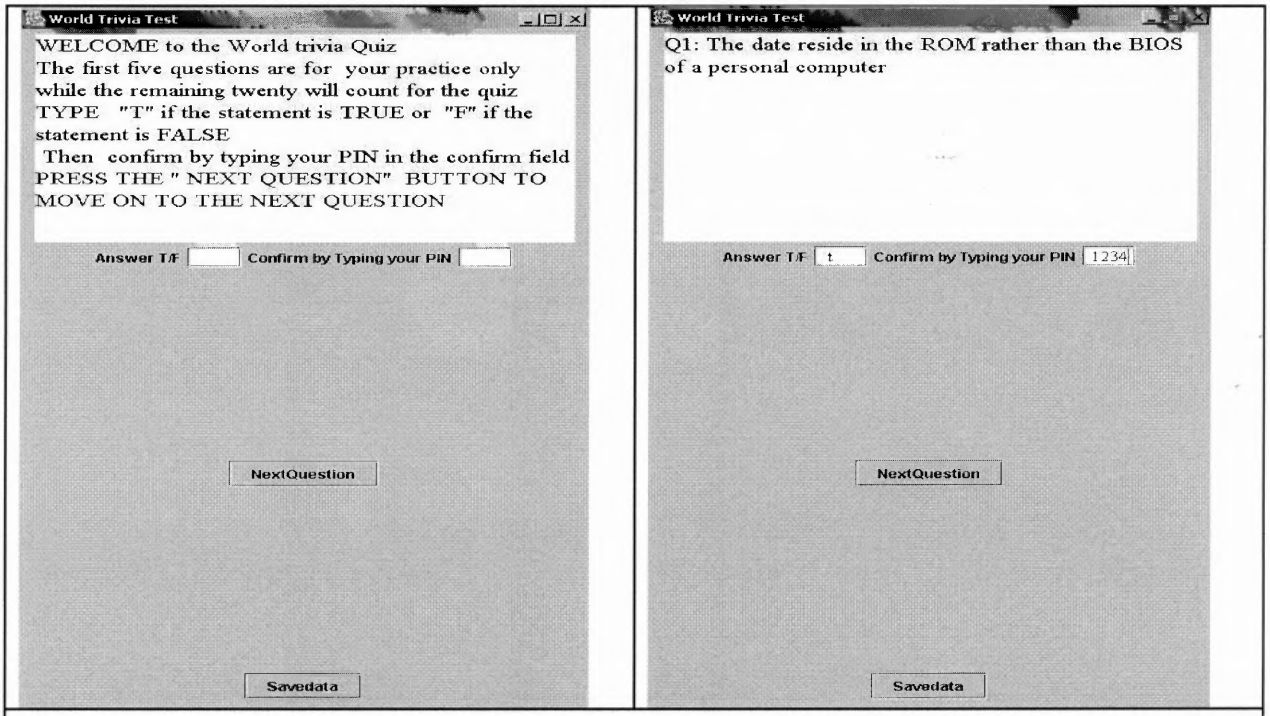

Figure 4.2 The world trivia welcome and question screens

The subjects then proceeded to the actual quiz and answered twenty five world trivia questions. The world trivia questions are shown in appendix O. The answer of each question was either true of false followed by a confirmation PIN entry. Data was collected from each subject using a pressure-sensitive keypad that was a modification of an existing keyboard. A lab-view software product was used to sample data from this keyboard. The data was then saved as a text file for each subject trial to be processed later. The details of the data features extraction are given in the next section on the development of the prototype. Several steps were taken to avoid some of the given measurement errors; (1) All subjects were trained until they were proficient with the program and their time patterns were stable. (2) All subjects were given a world trial quiz instead of being asked for their typing patterns in a direct way. This was meant to distract subjects' attention from the mechanics of keying the PIN to the mechanics of

answering the questions correctly. This ensured more natural patterns as users would use the recall part of the brain (cerebellum) when typing the PIN recall motion rather than the frontal cerebrum. (3) Subject answered twenty five world trivia question but the first seven were discarded on the assumption that they were not yet stable. (4) Subjects were instructed to use the number pad and not the top keyboard row of numbers. This reduced variability from different keys. (5) The system was such that there would be feedback if the subject typed the wrong PIN. The data with errors would be discarded. (6) All the subjects were instructed to use the forefinger of their dominant hand to type in the PIN number on the keypad. (8) The keyboard was set at an angle of 15 % from the horizontal level of the desk using the keyboard lever. (9) All the experiments were done using one adjustable chair that was always adjusted for each subject so that their elbows were level with the biometric keyboard. (10) The laboratory in which the experiments were performed was a quite environment with only two other users. This minimized disturbances. Care was also taken to make sure the lights in the laboratory were on to ensure sufficient lighting.

The keyboard that was used was a Microsoft extended keyboard model EO6401852. The diagram below is a demo of the process. The top of the illustration shows the subject pressing the first two keys of the personal identification number and the first two voltage signals produced from pressing the first two keys of the PIN. There will be four such signals by the time the four PIN digits are all pressed. The key-down-time was computed as the time from when the rising waveform passed the first trigger voltage all the way to the time the waveform reach the peak and then fell down again below the second trigger voltage. The key-down-times are labeled in the illustration

above as K_1d and K_2d for the first and second PIN key respectively. The inter-key-time was computed as the time from between the fall of one PIN digit below the second trigger voltage to the time that the next PIN digit voltage rose above the next trigger voltage. It is labeled as K_{12} in the illustration.

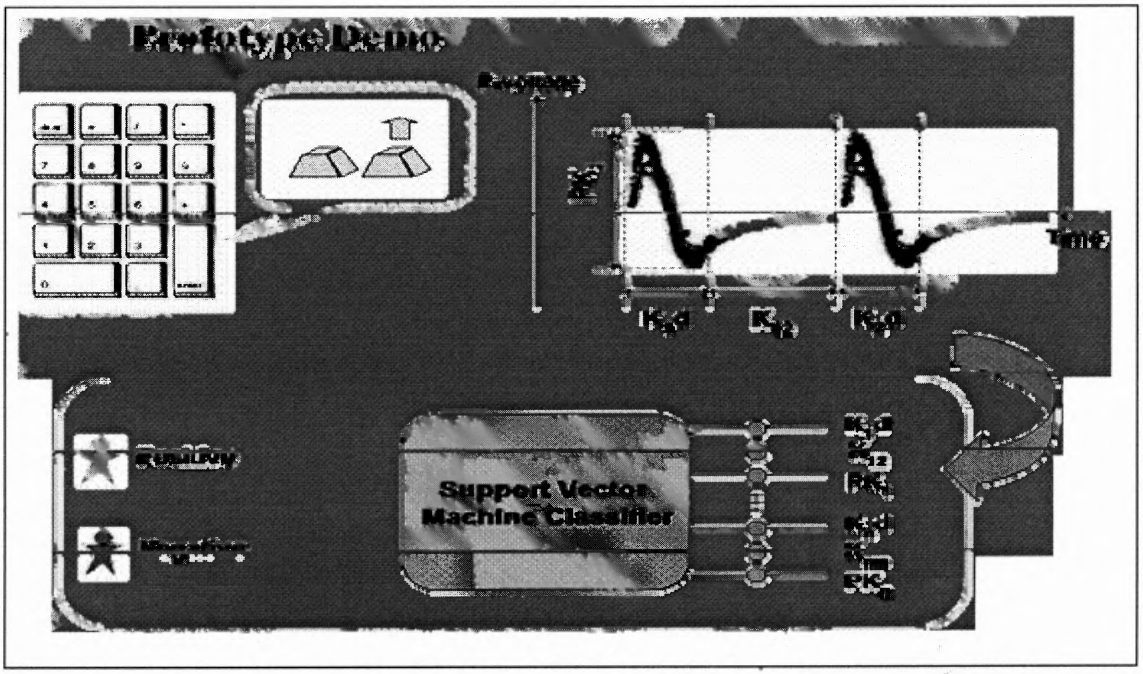

Figure 4.3 Illustration of the classification process

As the subject presses the keypad, voltage signals are generated by pressure sensitive resistors below the keypad. The key-down-times (K1d and K_2d) and the inter-key-time (K_{12}) and the wavelet coefficients are then computed and fed into the SVM classifier which compares this to the patterns of the user generated during training to arrive at a positive or negative verification decision.

The pressure signal produced during the key-down time is taken through a wavelet analysis toolbox to produce wavelet coefficients. These coefficients, the key-

down times and the inter-key time are then fed into an SVM classifier which compares this to the patterns of the user generated during training to arrive at a positive or negative verification decision. The details are in next section.

This section has so far presented the experiment task used to capture data and also given an overview of the classification procedure to give the reader the broad picture. The rest of this chapter will get into the details of data processing.

4.5 Development of the Biometric Keypad

This section assumes that the keys have already been pressured as shown in above demo. The voltage signal produced by the pressure sensor when hitting each key was sampled at a rate of 300 samples per second across the resistors under each key digit. This voltage was passed through an amplifier installed inside the keypad. The output from the amplifier was then connected to a standard laptop through an adapter board. The voltage was captured into the laptop by Labview software and saved as a text file. (Labview software from National instruments facilitates the interfacing of external hardware to computer systems and converts analogue signals to digital signals that can be processed and analyzed by a computer). The voltage across each key digit was monitored separately for each key. Thus, the raw data in the text file was made up of different chunks of data corresponding to the data streams captured from different keys. A Java program (whose pseudo code is shown in Appendix J) was used to separate and process the data chunks. This provided single continuous waveform data streams for each key for a total of four data streams for the PIN number. Each data stream had voltage pulses at points where

the key digits were pressed down. The other sections oscillated around zero at all other times when sampling was still occurring at times when the key was not being pressed.

The next step involved separating the keystroke voltage pulses from noise. This was done via the Java program (working steps shown in Appendix J) by use of two trigger voltages. The first trigger voltage detected the point at which the pressure voltage amplitude rose above the random noise. The trigger voltage was empirically determined by plotting the pressure voltage signals and choosing a point 0.01 mV above the noise maximum voltage. For example, if the maximum noise voltage was 0.05mV, then the trigger voltage would be computed as 0.01 +0.05 =0.06 mV. The same principle was used to determine the second trigger voltage which detected the point after which the pressure voltage signal gradually damped off into noise. It was also chosen to be 0.01 mV above the damped noise signal voltage, typically 0.05mV.

4.5.1 Wavelet Transformation

The above subsection explained how the inter-key time and the key-down times were computed. This subsection will explain how the wavelet coefficients were produced from the voltage signals.

The initial analysis used the pressure amplitude labeled as PK_1 as the appropriate pressure feature. However, an analysis of the state of the work in signal processing literature presented in Chapter 2, Section 6, revealed that using a wavelet transformation of the voltage signal results in wavelet coefficients that are better classification features than using geometric waveforms or Fourier transforms.

The first step in doing a wavelet transformation was to get the base signal waveform. This was done by extracting the voltage values of the waveform for the full key-down-time (i.e. values between the first and second trigger values for each key digit). The pressure signal values were then stored as a vector which was then fed into a wavelet analysis toolbox in Matlab™ (Misiti et al. 2004). The base signal was repeatedly decomposed into a high frequency and low frequency portions as explained in the theory section of wavelet analysis in Chapter 2, Section 2.9. This produced wavelet coefficients which were used for discrimination. The level of decomposition is the number of times that a signal has to be split into a high frequency and low frequency portion. This was determined empirically for this dissertation by computing the maximum number of voltage values in key-down-time that is also a power of two (Misiti et al. 2004). An analysis of the subject key-down times showed that most of the pressure key patterns lasted for less than one hundred and twenty eight milliseconds, hence the signals were all padded by zeros to be of size one hundred and twenty eight. The lever of decomposition was found by computing the power of two that would give one hundred and twenty eight which was seven. Thus the level of decomposition for this dissertation was seven.

4.5.2 Development of Neural Network Classifiers

Once the time and pressure features for pattern classification were acquired, the next step was to build a classifier for separating the test patterns into their appropriate classes.

The literature review in Chapter 2, Section 2.6.4, gave the rationale for short listing the neural network and support vector machine classifiers as the two candidate types of classifiers with the highest potential.

In cognizance of the above fact, a neural network classifier was the initial choice. A three layer neural network was designed and tested. However, the neural network classifier had the following shortcomings. The first shortcoming was that the determination of the neural network classifiers parameters (number of hidden layers, learning rates etc) was through a set of heuristics derived from standard pattern recognition books (Fukunaga 1990). The resulting classifier would work well for the given data but get unstable when the inputs changed. The second shortcoming was that the neural network classifiers took too long to train especially with an increasing number of subjects. Further the classifier performance fell off sharply with an increasing number of samples. A decision to move to support vector machines (SVM) classifiers was made. The next subsection gives the development of the SVM classifier.

4.5.3 Development of Support Vector Machine Classifiers

The literature review in Chapter 2, Section 2.6.6, gave the theory behind support vector machines. The section demonstrated that support vector machines are a relatively new method of pattern classification compared to other methods like neural network. The SVM method is powerful and has been shown from previous research to outperform most of the other pattern recognition methods (Cortes and Vapnik 1995).

The four popular kernels functions used by SVM classifiers were considered. These are the linear, polynomial, radial basis function and the sigmoid kernel functions. The radial basis function was chosen as it can handle both linear and non-linear vectors and has a superset of most of the characteristics found in the other three kernel functions named above (Hsu et al. 2003).

The next step was the implementation of an SVM classifier. There are several support vector machine engines in the computer science research community which could solve the problem in this dissertation. The OSU SVM Matlab™ toolbox (Ma et al. 2005) was chosen as the best engine due to its popularity and the availability of tutorials on the configuration and design development .The typing patterns were then rearranged to fit the format required for the above toolbox. The steps used in preparing and formatting data to fit this module and execute the rest of training and testing steps followed those recommended by (Hsu et al. 2003). The steps were (1) Transform data to the format of the SVM software, (2) Conduct simple scaling, (3) Consider using the RBF kernel, (4) Use cross-validation to find the best parameters C and γ, (5) Use the best parameters to train the classifiers. (6) Test the classifier.

Three set of classifiers were designed and built in Matlab™ each using OSU SVM Matlab™ toolbox classifier engine. The following paragraphs detail the operations carried out in each of the above recommended steps

The data did not need to be transformed as the seven dimensional time features data vector and the four dimensional wavelet coefficients vector were already in a format required by the SVM toolbox. However, the data was scaled to the range (-1,1) to avoid domination by either the time or the pressure vector on the other and to make numerical computation easier (Hsu et al. 2003)

The next step was to compute the optimal parameters for the SVM classifier and investigate the optimal classification rate. The SVM best practice steps given above recommended the use of the radial basis function as the kernel function for transforming the data dimensions to a higher dimension to ease separation. There are two important

parameters for the radial basis function (RBF) kernel based SVM classifier (C, γ) which determines the performance of any RBF classifier. To get the best parameters for the classifiers used in this dissertation, a grid search method was performed over the pairs given below as recommended by (Hsu et al. 2003).

Table 4.2 Grid Search Values used for Determining Optimal RBF Parameters

C-values used =

[-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25]

Gamma–values used were

[-15,-14,-13,-12,-11,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,11, 12,13,14,15];

γ =2^GammaValues(i), C= 2^CValues(i);

A program loop was designed in which pairs of corresponding values of (C, γ) were picked from the set given above and each time the average classifier performance would be determined by cross-validation method. In the cross-validation method, data would be divided into k-folds (k=4 was used most of the time) and the classifier would be trained on the k-1 subsets and tested on the k-fold. K would then be shifted forward and the same process repeated until the last fold. A graph of the classifier performance was plotted and the RBF kernel parameters in which the best performance was achieved were noted. For this dissertation, the optimal values were found to be (2048, 2) and the best classification rate obtained for the four PHD students was 90%. This showed that the biometric keypad method was technically feasible but could not be used as a stand alone method as this classification rate was not high enough.

4.6 Result of Technical Feasibility Investigation

The successful development of the biometric keypad was an important milestone in the dissertation process. The theoretical investigations done in Chapter 2, Section 2.9 on developing a keyboard-based classifier and the work done in this chapter addressed the four research sub-questions as follows.

The first research sub-question sought to find out if individual typing patterns for a numeric keypad using a small (4-6 digits) number for authentication would be unique. This question was answered in two stages. The first stage was in the theoretical review section where it was suggested that in general , the latencies between successive keystrokes, keystrokes, durations, finger placement and applied pressure on the keys can be used to construct a unique user signature/profile (Monrose and Rubin 2000). This general answer was from experiments using a lot of text. However, this dissertation was investigating whether this could be extended to the 4-6 digits case. The fact that the biometric keypad could produce classification rates of 90% using a four digit PIN implied that the case was also true even for this number of digits although the classification rate was not as high compared to some previous work rates of 95% etc. This mean that the 4 PIN authentications could work as a second layer to the other authentication systems but may not work as a primary layer which was in agreement with the proposed solution for identity fraud where the biometric keypad was to be applied as a second layer.

The second sub-question sought to investigate what would be the best classification features to use for the biometric keypad. Several candidate features were extracted from the previous work. It was shown in Chapter 2, Section 2.91 that the inter-

key time and the key-down-town were the best two features to use as they retained the most information. This chapter demonstrated the implementation of such a solution to obtain reasonable classification rates which confirmed the above for the biometric keypad.

The third sub-question sought to investigate the best classification method. The preview of previous works in Chapter 2, Section 2.9.4 analyzed several classifiers like Bayes, linear classifiers, parametric classifiers, neural networks and support vector machines. The literature helped narrow down the list to two candidates namely the neural network and the support vector machines. This chapter implemented the neural network and encountered several problems as explained in section 4.5.2. A decision was made to move to support vector machine with which a classification rate of 90% was attained. This means that the best classifier for the biometric keypad is the support vector machine used with the optimal parameters that were also determined by this dissertation.

The fourth research sub-question sought to investigate how the biometric keypad could be built to sample both pressure and time data. The implementation shown in the prototype section above and the development section can serve as a template/starting point for future implementers of biometrics.

A summary of this results are given below. This table will be developed for all research questions in the course of the dissertation chapters till complete.

Table 4.3 Answers to Research Sub-questions 1-4

No.	Research sub-questions to be investigated	Answer to research sub-question	Source	
			Lit review	Stage 1 of Study 1
1	Are individual typing patterns unique for a numeric keypad using a small (4-6 digit) number for authentication?	Yes they are unique. Attained 90% classification from 4 subjects	Suggested	Confirmed for 4 digits
2	What are the optimal characteristics of the input signals that should be used for classification of different users?	Inter-key time, key-down time and wavelet coefficient	Suggested	Confirmed
3	What method is best for characterizing the pattern differences produced by individual typists?	Support vector machine	Suggest Neural network and SVM	SVM confirmed to be superior
4	How should a pressure keypad be built and sampled to provide pressure data to the classifier engine?	Follow the biometric keypad template		Designed & implemented template

4.7 Summary

The main objective of this chapter was to test the technical feasibility biometric keypad; i.e. find out if the biometric key pad has reasonable classification rate and optimal parameter for attaining such a rate. The chapter started by introducing the modules of the biometric keypad and then explained each module. The subjects and the procedures used were then given. The chapter ends by presenting and discussing several findings that resulted from the study.

CHAPTER 5

RESEARCH METHODOLOGY- RQ1: TECHNICAL FEASIBILITY

5.1 Introduction

This Chapter addresses stage two of Research Question 1. It examines the performance of the classifier developed for the biometric keypad under two possible conditions that are likely to occur in its everyday use. The first is elapsed time between keypad entry and the second is type of keying pattern used. As such, this chapter describes an experiment which varies these conditions and measures the classifier effectiveness for each of the variations.

The chapter is organized as follows. It first gives a quick overview of prior typing research that was presented in Chapter 2 in order to develop the theoretical foundations for the hypotheses used in the experiment. It then describes the experiment design followed by a description of the subjects used in the study and then the procedures that were used. Following this is a description of a post hoc analysis to be run to address one of the research questions posed in stage one of this evaluation of the technical feasibility of a keypad biometric, that is, whether the addition of pressure adds to the effectiveness of the classification. This is followed by a description of a second post hoc analysis that looks at whether typing skill affects classification rates. Typing skill was included in the experiment design as a covariate because it was known to affect the other variables. It was not used as an additional factor because the number of subjects was low and the other two factors were of primary interest.

The experiment described in this chapter will address the sub-questions in the table below that were posed in Chapter 3 which presented the research design of this dissertation. The numbers used in Chapter 3 are preserved.

Table 5.1 Research Sub-Questions 6-9

No.	Research sub-questions
6	Would the addition of pressure pattern features to the time pattern features improve discrimination accuracy?
7	How much will variations in typing speed impact classification performance?
8	What is the effect of elapsed time on the classification performance?
9	Are there differences in classification performance for different pin numbers?

Questions number 6 and 7 will be addressed by post hoc analyses conducted at the end of the experiment. Questions 8 and 9 will be part of the experiment design. The literature review in Chapter 2 looked at studies that measured keyboard learning over time. The studies indicated that skilled motor performance involves continuous learning so that we can expect users to get better and better at typing in their password or PIN number. The studies also indicated that there were significant changes in the distribution of inter-key times as a person gained expertise suggesting that a classifier might not continue to work as a user typed in their PIN number over time. Additional work on typing performance over elapsed time showed that the performance was different depending on the elapsed time interval. Although no work exists on the effectiveness of a classifier over time and over different elapsed time intervals, typing research suggests that this variable needs to be considered.

Thus, the first hypothesis to be tested in this experiment is:

H1a: Keying patterns with elapsed times of one week and one month will have significantly different and lower classification rates than those of the keying patterns used to develop the classifier.

The research on typing performance reviewed in Chapter 2 also indicated that higher variance existed for some key digraphs than for others. In addition, the letter context of a key pattern was found to have an effect on inter-key times. However, it was not known if this context would affect the variance of these inter-key times and thus, impact classification effectiveness. This leads to the next hypotheses to be tested in the experiment.

H1b: There will be a significant difference in classification rates between the PIN, 1234 and the PIN, 1324 with PIN 1234 showing lower classification performance.

The above hypothesis is directly related to the experiment design which selects only two versions of PIN numbers to test. A more thorough study looking at impact of multiple combinations of keys could be run in the future to look at the impact of key distance and context on classification rates, but this dissertation is focused primarily on learning whether there is an impact so the above two combinations were chosen to represent different initial and final key distances that are likely to affect classification.

Research sub-question number 7 addresses the impact of typing skill on classification. Since the literature reviewed on typing indicated that typing skill affected both how learning performance and the inter-key time variability for different digraphs, it was decided to use typing speed as a covariate for the other two conditions manipulated

in the experiment, elapsed time and PIN pattern and to analyze it separately in a post hoc evaluation after the study. The next section presents the design of the experiment.

5.2 Experiment Design

A 3 X 2 factorial design was used to build the experiment using the independent variables elapsed time (day of trial 1, 1 week after trial 1, 1 month after trial 1) and PIN pattern ("1234", "1324"). Elapsed time period was treated as a repeated measure. The dependent variable was classification rate, that is, the percentage of correctly classified patterns. Typing speed was used as a covariate in the study. Table 5.2 presents a summary of the design.

Table 5.2 Summary of Experiment Design

		Levels	Conditions
Dependent variable	Classification rate	Continuous	0-100%
Independent variables	Time periods	3	1day 1week 1 month
	PIN combination	2	PIN1234 PIN1324
Covariate	Typing experience	Continuous 10 – 70 wpm	

5.2.1 Description of Subjects

The subjects who participated in the biometric keyboard experiment were from a class of undergraduate students in an East Coast U.S. university. Twenty-four subjects participated in the study. All were enrolled in a computer-based program at the university and were in their 2nd or 3rd year at the university. Subjects ranged in age from 18 -33 with a median age of 22 years. 25 percent of the subjects were female and 75 percent were male. All subjects had significant prior experience using an ATM machine (i.e., greater than 12 month). The subjects on average used computer for 69 hours a week

with a standard deviation of 2 . Their mean typing speed was 35 w.p.m. with a standard deviation of 16.9. All were right handed.

5.2.2 Experimental Procedures

The subjects were randomly divided into two groups, the first one given PIN "1234" while the second group was given PIN "1324". Each group participated in the three repeated trials using the assigned PIN

The subjects in each group were first asked to sign a consent form and then fill a pre-test questionnaire which requested subject demographic data. The consent form and the pretest questionnaires are shown in Appendix B and C respectively. The subject would then be taken through a typing test. The typing test consisted of typing a single passage using freeware software from the WEB. The typing duration and speed would then be recorded.

The subject would then be trained on the experimental task. The training consisted of answering world trivia questions followed by typing of the allocated personal identification number until they felt confident and their patterns were stable. The diagram below shows the world trivia screen.

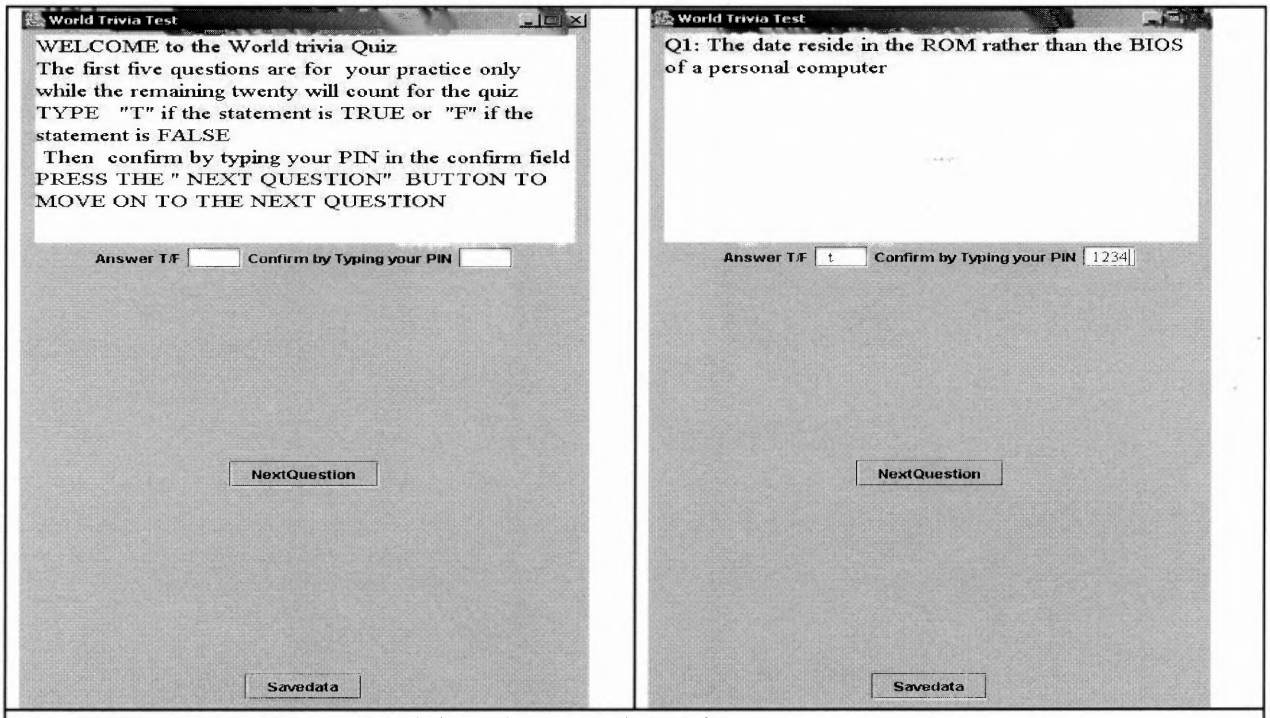

Figure 5.1 The world trivia welcome and question screens

The subjects then proceeded to the actual quiz and answered twenty five world trivia questions. The answer of each question was either true of false followed by a confirmation PIN entry. Data was collected from each subject using a pressure-sensitive keypad that was a modification of an existing standard keyboard. A lab-view software product was used to sample data from this keyboard. The data was then saved as a text file for each subject trial to be processed later. The details of the data features extraction are given in Chapter 4 on the development of the prototype. Several other steps were taken to avoid some of the given measurement errors; (1) All subjects were trained until they were proficient with the program and their time patterns were stable. (2) All subjects were given a world trial quiz instead of being asked for their typing patterns in a direct way. This was meant to distract subjects' attention from the mechanics of keying the PIN to the mechanics of answering the questions correctly. This ensured more natural

patterns as users would use the recall part of the brain (cerebellum) when typing the PIN recall motion from the memory rather than the frontal cerebrum. (3) Subject answered twenty five world trivia question but the first seven were discarded on the assumption that they were not yet stable. (4) Subjects were instructed to use the number pad and not the top keyboard row of numbers. This reduced variability from different keys. (5) The feedback system was such that there would be feedback if the subject typed the wrong PIN. The subject would then be asked to repeat the task. (6) All the subjects were instructed to use the forefinger of their dominant hand to type in the PIN number on the keypad. (8) The keyboard was set at an angle of 15 % from the horizontal level of the desk using the keyboard lever. (9) All the experiments were done using one adjustable chair that was always adjusted for each subject so that their elbows were level with the biometric keyboard. (10) The laboratory in which the experiments were performed was a quite environment with only two other users. This minimized disturbances. Care was also taken to make sure the lights in the labs were all to ensure uniformity. The keyboard that was used was a Microsoft extended keyboard model EO641852.

The subject was then thanked and requested to come back and repeat the same task after approximately one week (after 6-8 days) and approximately one month (after 28-32 days) respectively. The same procedures were run in the one week after and one month after session.

5.3 Post Hoc Analyses

Two post hoc analyses are planned for this experiment. They are post hoc analyses not because they are an afterthought of what might be investigated, but rather because the design and collection of the data in the experiment precluded these investigations being part of the experiment plan. The first of these investigations is that of the impact of using the pressure features to enhance classification. Because the subjects knew nothing about what type of information was being captured for discrimination and because the modifications made to the keyboard to capture pressure did not impact subject performance, it is reasoned that the data collected for other measures in the experiment will not affect this analysis.

To perform the comparison for the pressure impact analysis, the classification rates will be calculated for three conditions for each cell in the experiment. Only classification rates within each cell will be compared. The three conditions will be (1) classification rates calculated using time features only, (2) classification rates calculated using pressure features only, and (3) classification rates using both time and pressure features. It is planned to randomly sample two-thirds of the data in each cell for training the classifier and then to use the remaining third of the data to calculate the classification rates for each subject. This procedure will be done fifty times, and an average classification rate will be calculated for each subject in the cell and for each cell. These classification rates will then be compared through an analysis of variance for each of the three conditions.

The second of these post hoc investigations is that of determining the effect of typing ability on the classification rates. Typing speed for each subject will be measured

through an online typing speed program for each of the subjects. Because typing skill is likely to interact with classification rates and because it was not used to assign subjects to cells, this typing speed will be used as a covariate in the statistical analyses to be run on the independent factors in the experiment. Typing speed impact will also be investigated by conducting a regression analysis to determine if typing speed is correlated with classification rates. It is hypothesized that it is linearly correlated with classification rates up until typing speed reaches approximately 30 words per minute. This is the threshold at which typists become "touch" typists. It is felt that at this threshold, typing becomes more uniform and consistent so that discrimination is easier making classification rates rise.

5.4 Summary

The chapter started by presenting the objectives of the biometric keypad evaluation. Several research sub-questions formulated in Chapter 3 are given and corresponding hypothesis proposed. The demographics of the subjects who participated in the experiment are presented followed by the design of the evaluation experiment. Various steps that were taken to address reliability are addressed followed by the design of two proposed post hoc analysis.

CHAPTER 6

RESULTS FOR RESEARCH QUESTION 1: TECHNICAL FEASIBILITY

6.1 Introduction

This chapter presents the data analysis performed on the data collected from the experiment described in Chapter 5. The chapter starts by describing how the dependent variable, classification rate, was constructed from the raw data collected from each subject trial. This is followed by a presentation of the results from a two-way ANOVA run using classification rate as the dependent variable with time periods (as a within-group variable) and the two personal identification numbers (as a between group variable) as the independent variables. A discussion of the implication of these results on the technical feasibility of the biometric keypad follows each factor's analysis.

Following the analysis of variance presentation are two post hoc analyses, which examine the effect of two other factors that are relevant to the design of the keypad biometric. The first of these is typing skill. The second is the addition of the pressure parameter. Since typing skill was used as a covariate in the analysis of variance, and since it was collected as a random variable that does not cover the full range of typing skills, a post hoc analysis is preferred, in particular, since this examination is primarily to capture what real life variations might have important impacts on the keypad biometric technology. That is to say, the experiment conducted was to uncover a collection of potential variables that would affect the performance of the classifier with the intent of exploring further those variables that indicated an impact.

Pressure is examined as a post hoc consideration for the following reason. Although the effect of pressure was examined in the development of the classifier, this

development only used 4 subjects. Thus, it is useful to reexamine the advantage pressure provides in classification accuracy with data generated by the twenty-four subjects in the experiment. A discussion follows each of the resulting post hoc analysis relating them to the technical feasibility of a keypad biometric. Finally, a summary section is given which focuses on how well this chapter provided answers to Research Sub-Questions 6-9.

6.2 The Impact of Elapsed Time and PIN Design on Discrimination Accuracy

Two hypotheses were predicted in Chapter 5. They are:

H1a: Keying patterns with elapsed times of one week and one month will have significantly different and lower classification rates than those of the keying patterns used to develop the classifier.

and

H1b: There will be a significant difference in classification rates between the PIN, 1234 and the PIN, 1324 with PIN 1234 showing lower classification performance.

An interaction effect is not expected between these two variables. Such an interaction effect would imply that our subjects will change their typing of one PIN number significantly after an elapsed time period and not change their typing of the other PIN number as significantly. Nothing in the literature on typing suggests this, in particular, since the PIN numbers are both numeric and the keys close to each other on the keypad. It may be that certain typing patterns are more difficult to learn, but PINs are expected to be approximately equal in learning performance.

6.2.1 Algorithm Used to Develop Dependent Variable

The following algorithm was used to develop the classifier for the first (PIN= "1234", time period 1) and fourth (PIN = "1324", time period 1) cells of the factorial design. First, the first seven trials were discarded as unstable. Two-thirds of the remaining keying pattern data were then randomly selected and used to train an SVM classifier while the remaining one-third was used to test the classifier. This training and testing was repeated using a bootstrap algorithm for 200 iterations while randomly selecting another two-thirds, one-third combination. After each iteration of the bootstrap algorithm, the classification for each subject was examined and given a score of 1 (successful classification) or 0 (unsuccessful classification). At the end of classification, each subject had a score of the number of successful evaluations to the total number of evaluations. This was normalized to a value between 0 and 100 and used as a measure of the classification rate for each subject. It was this classification rate that was then used as the dependent variable in the experiment. The classifier trained in time period one was then used to test the data from time period two and time period three in a similar bootstrapping procedure. The same process was repeated for the second group of data for PIN= "1324" with the classifier developed in Time 1 for this PIN being used.

The above tests resulted in 200 classification rates values for each of the six cells of the factorial design table. The mean of each subject classification rate and its standard deviation for each cell was computed as shown below.

Table 6.1 Mean and Standard Deviations of Classification Rates for the Six Cells with the Standard Deviation for each Cell is Shown in Parenthesis

	Time period 1	Time period 2	Time period 3
PIN = "1234"	83.52 (15.7)	15.84 (37.1)	8.33 (28.9)
PIN = "1324	83.26 (13.2)	28.22 (37.7)	22.72 (32.9)

As can be seen from the table, there is a considerable degradation in classification rate over time. This degradation is worse for the "1234" PIN than for the "1324" PIN. A two way ANOVA was then performed on the mean classification rates for each subject using a mixed model of within subjects (elapsed time periods) and between groups (PIN number). The typing speed for each of the subjects was used as a covariate in the analysis. The results confirmed hypothesis H1a, namely that there is a statistically significant effect of time periods ($F(2, 71) = 49.98$ $p > 0.001$) on the ability to classify individuals. The second hypothesis, H1b was only tending towards significance ($F(2, 71) = 2.3$, $p = 0.065$). Thus, with the twenty-four subjects, the experiment was not able to uncover any differences in the PIN number construction that affected classification rates. As expected, there was no interaction effect between PIN number and elapsed time period ($F(2, 71) = 0.57$, $p = 0.28$). It should be noted that before typing speed was used as a covariate, a significant effect was found for PIN number differences indicating an interaction between typing skill and PIN number design, i.e., some PIN numbers may be harder to classify for weak typists because of large variations in their "hunt and peck" method. This issue will need to be explored further in future studies.

6.2.2 Discussion of the Impact of Elapsed Time on Classification Accuracy

The important question addressed with hypothesis H1a was whether the classification accuracy would change across the different elapsed time periods. The results from the two-way ANOVA show that they change significantly. The descriptive statistics table showing the means for each of the time periods indicates that the classification accuracy is worse for an elapsed time of one month than for one of one week. The implication is obvious. Any keypad biometric built using a classifier developed using the first initial mass practice group of data (e.g., when a customer first selects or is given a PIN) is not likely to work effectively a short or long time later.

This result can be explained by the discussion on how people acquire motor skills that was presented in Chapter 2, Section 2.10.1. As the subject learns to type the PIN, the time to type the PIN shortens. With each subsequent practice session, the PIN typing times continue to decrease. A known reason for this decrease in typing time is a decrease in inter-key times. This decrease has been found to not occur consistently for all keys. The effect of this reduction in duration is a decrease in classification performance because the new typing patterns do not match the patterns used to train the classifier in time period one. Thus the model developed during training becomes more and more irrelevant, leading to deterioration in classification performance.

One way of addressing changes that occur over time is to conclude that the biometric keypad is not appropriate for use in authentication systems. Another solution is to design for the change in patterns over time. Part of this solution would be to capture keying data only after an individual has used a PIN number for some threshold level of times, e.g., 50 times. A second part of the solution would be to capture keying data in

situ and not in a mass practice session since it is known that mass practice degrades performance. The third part of the solution would be to make the algorithms self-adjusting such that the algorithm retrains on new data to keep the classifier current with the changing patterns of the user. Such a self-adjusting algorithm will need to be tested in subsequent studies. A useful part of the current experiment is that it provides useful data on what typing behavior is changing that affects the classification rate.

The next section addresses the non-significant result from the second hypothesis that predicted that different PIN configurations would impact classification accuracy.

6.2.3 Discussion of the Impact of PIN Design on Classification Accuracy

This section discusses the results of the PIN main effect. The study had hypothesized that the group having PIN ="1324" would have a higher classification rate than the group having PIN = "1234". The experiment did not find a significant difference between the two pins, but the level of significance was close to the p = 0.05 level. A review of the literature had indicated that different typing sequences had different variances in inter-key times, one of the parameters used by the classifier. The first PIN = "1234" has three digits that are next to each other on the keypad and are typed in a continuous sequence from left to right. The fourth digit is a return to the first column and a transition to another row. The PIN = "1324" has digits in which the typing sequence requires jumping from "1" to "3" and then going backward to get "2" followed by a jump from the keypad row containing "123" to the row containing "456". Because the typing moves from key 1 to key 2 to key 3 are more consistent, it is expected that these keys will show up less variation between users than the key jumps in the second PIN. Thus, the PIN "1324" was

predicted to be easier to classify. The failure to get a statistical difference could be for several reasons. First, the effect size is small and therefore, the test did not have enough power to reject the null hypothesis because of the low number of the subjects. Another possible reason considered is that the PIN = "1234" was easier to learn so that typing patterns were more consistent over time canceling out the effect of less user variation. However, no significant interaction effect between PIN design and time period was found suggesting that if this is a reason, it also was a small effect that could not be captured. The best guess is that the effect size is small because the key travel distances for the two PINs were not very different. Larger key travel times are likely to have larger effects on classification accuracy. This is definitely suggested by the nearly significant results.

6.3 Post Hoc Analysis on Typing Speed and Pressure Measures

This section gives the analysis of factors that were not controlled in the experiment but which were also of interest. A key reason for not adding typing speed as an experimental factor was the limited availability of subjects and no a priori information on what level of typing speed might have impacted classification accuracy. In addition, although students in computer-related fields spend large amounts of time at computers, they tend not to be touch typists so that their typing speeds would fall mostly in the lower ranges making it hard to build a factor based on high and low typing speeds. Typing speed could also have been treated as a random variable, but pilots suggested interaction effects that would have made it more difficult to tease out results for the other variables. Thus, typing speed was used as a covariate in the study and is analyzed below. The analysis of pressure is a validation of the analysis that was carried out on four subjects in the validation of the

classifying algorithm. Data from twenty-four subjects is a better test of any advantage gained from using pressure as a classification parameter and thus, forms a better validation of its use.

6.3.1 Correlation between Discrimination Accuracy and Typing Speed

Typing speeds were measured after the assignment of the subjects to cells. This was done by asking students to type a relatively easy paragraph of 276 characters of prose in an online typing program called Typing master (Typing Master Finland Inc. 2002). To determine if typing speed affected classification accuracy, a correlation was calculated between classification rate and typing speed for each subject for PIN = "1324". The rest of this section describes the algorithm used and the results obtained.

The average classification accuracy rate obtained for each of the 12 subjects for PIN = "1324") over 200 bootstrap runs was computed. Each subject's typing speed was plotted against the corresponding average accuracy as shown in the figure below (The actual data points shown by "+" points.) A regression was fit to these points. The line in the figure shows the regression line. A table of results showing the intercept and slope of the regression follows the figure.

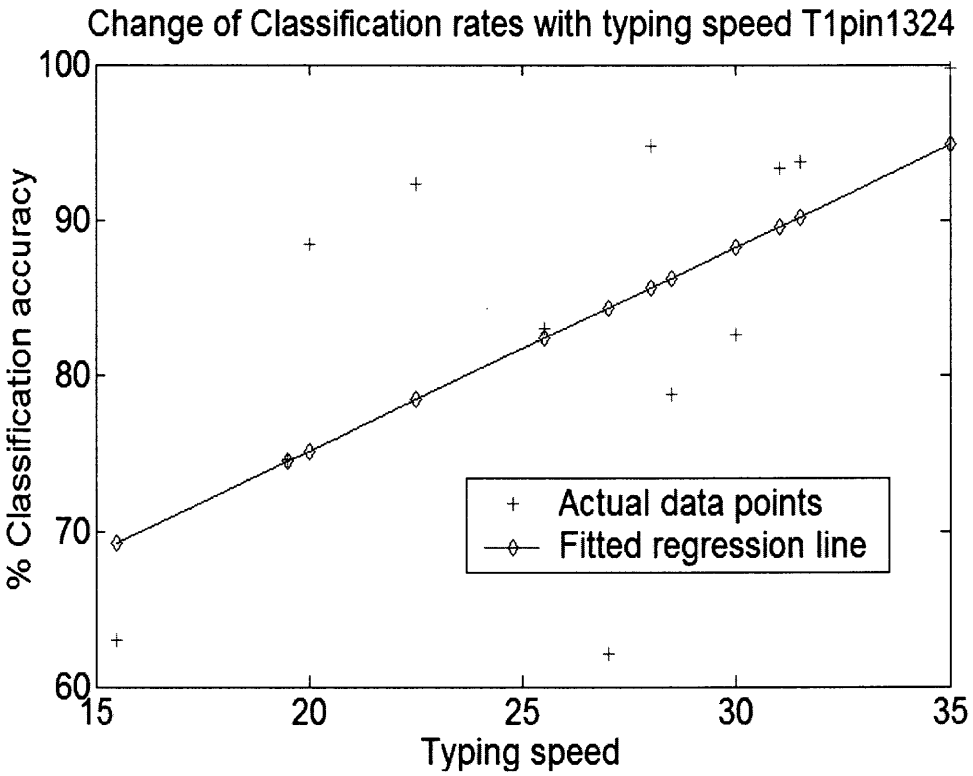

Figure 6.1 Variation of discrimination accuracy with typing experience

Table 6.2 Parameter Estimates for Regression Line

Variable	Parameter Estimate	Standard Error	t-value	Pr>|t|
Intercept	48.9	15.9	3.07	0.01
Typing speed	1.313	0.59	2.21	0.05

The above table gives an intercept of the line as 48.9 which is statistically significant ($t = 3.07$, $p = 0.01$, $n=12$) and a slope of 1.313 which is also statistically significant ($t = 2.21$, $p = 0.05$, $n = 12$). Thus the equation for this regression is

$$y = 1.31x + 48.9 \qquad \textbf{Equation 6.1}$$

The implication of a significant regression fit is that there is a direct correlation between typing speed and accuracy. Thus, subjects with low typing speed have low

classification accuracy and vice-versa. The above observation implies that a biometric keyboard works best for experienced typists and gives below average classification rates for inexperienced typists. Research on learning to type shows high variability in inter-key times for the novice typist which also supports this result.

6.3.2 Comparison of Classification Accuracy With and Without Pressure

The second investigation of interest in this research that was not part of the factorial design was the effect of pressure on classification accuracy. Pressure was not a factor in the experiment because subjects were not aware that pressure was being recorded so its presence should have had no impact on the human performance. The approach taken in this post hoc analysis is to calculate classification rates for each subject using the pressure and time parameters, then to calculate these same classification rates using only the time parameters, and finally to calculate classification rates using only the pressure parameter.

To perform this comparison, three Support vector machine classifiers were trained on the time parameters, the pressure parameter and combined parameters respectively. Two-thirds of typing pattern data randomly selected from each subject was used to train the classifier and the remaining third was used for testing. The pattern sampling was then done again and the same process repeated until fifty bootstrap steps were completed. For each bootstrap process, a mean was obtained from the classification accuracy calculated for each of twelve subjects. For example, for Time Period 1 and PIN = "1234", there should be three means for the first iteration of the bootstrap calculation, one for time parameters only, one for both time and pressure parameters and one for the pressure parameter, only. The mean for each type of classifier manipulation was then plotted

against the bootstrap iteration. The figure below shows a typical plot of the performance for each parameter combination used. The plot shown is for the first experiment cell group (Time Period 1, PIN = "1234"). Other plots for other cells in the experiment were similar.

It is observed that the classifier using a combination of time and pressure features has the highest performance while the classifier with pressure features only has the lowest performance among the three. Since the normality requirement cannot be assumed for data coming from twelve subjects, a non-parametric statistical measure for comparing the means of three different sample means was used to determine if these visual differences were statistically significant. A Kruskal Wallis test comparing the three classifiers mean performances rates was performed. The test confirmed that the combined features classifier performed better that any of the other two classifiers. The difference was statistically significant. (χ^2 (2, 49) = 121.7, $p < 0.001$).

The results confirm the earlier assertion that the addition of pressure to the time features used in previous research on biometric keyboard classifiers results in better classification performance. The implication for this finding is that the pressure feature offers an additional advantage, which should be leveraged by designers wishing to attain better performance.

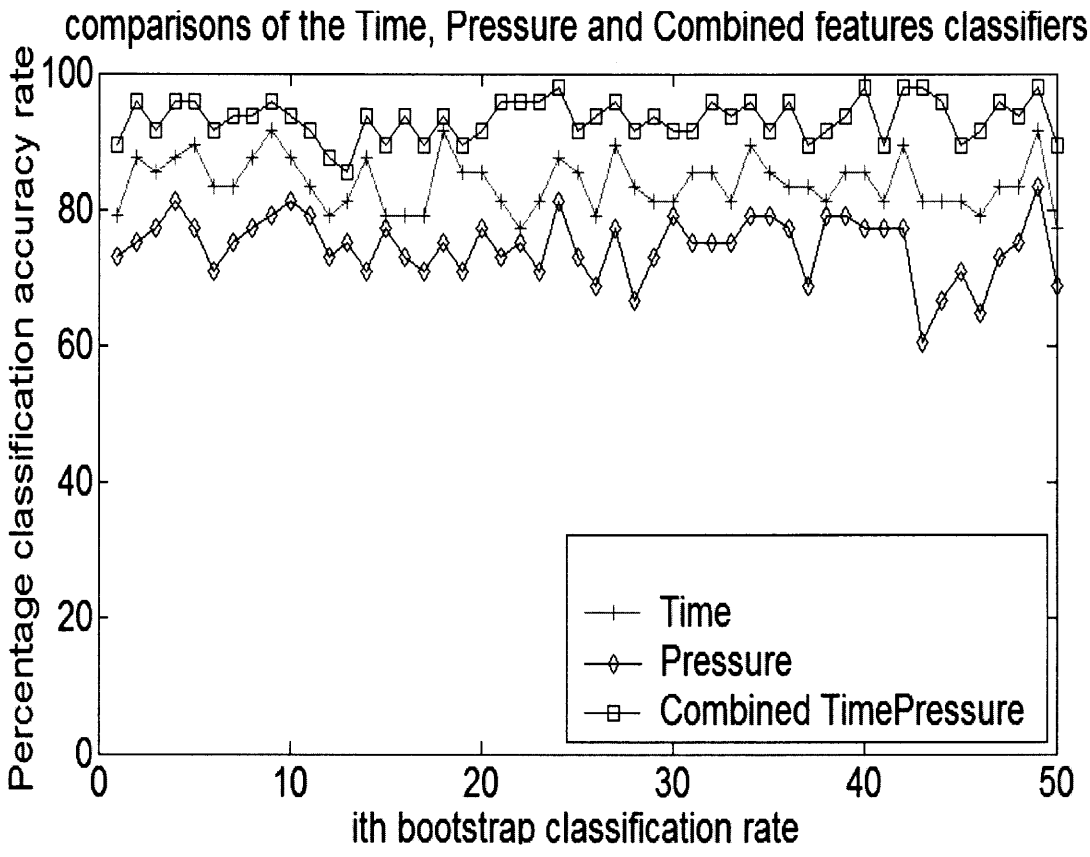

Figure 6.2 Comparison of time, pressure and combined features classifiers.

6.4 Summary

The analysis in this chapter has addressed four of the research sub-questions that are being investigated in the first portion of this dissertation, which examines the technical feasibility of developing a keypad biometric. The text that follows summarizes whether the analysis has succeeded in answering the sub-questions.

Research Sub-question 6: Would the addition of pressure pattern features to the time pattern features improve discrimination accuracy. The post hoc analysis and the significant statistical results indicate that adding pressure pattern features improves discrimination accuracy.

Research Sub-question 7: How much will variations in typing speed impact classification performance. The post hoc analysis developed a regression equation to predict classification accuracy from typing speed. Although at some point, typing speed is not likely to be a factor, it is clear from the significant fit and the relatively steep slope of the regression line that poor typists have a significant deleterious impact on discrimination accuracy. At about 30 words per minute, this seems to disappear, which is approximately where touch typing starts to take over "hunt and peck" typing. Thus, this question was answered, although more experimentation could be done in this area, possibly collecting a wider range of typing ability and fitting the data to an exponential function.

Research Sub-question 8: What is the effect of elapsed time on the classification performance? This question was addressed by Hypothesis H1a in the experiment that predicted that PINs typed in one week and one month after the system had been trained on an individual's typing pattern would have lower classification performance. Classification accuracy was found to drop significantly for these time period differences with a difference of one month having the worst performance. Thus, this research question was addressed, although the results show that the technical feasibility of the keypad biometric will require more difficult procedures that continue to retrain classifiers.

Research Sub-question 9: Are there differences in classification performance for different pin numbers? This research question led to hypothesis H1b which stated that classification performance would be poorer for PIN = "1234" than for PIN = "1324". No significant difference was found between these two PINs. It was noted that perhaps the

effect size was too small to show up with the number of subjects studied. It was also suggested that the keyboard distances traversed on a keypad were too small to affect subject variation and thus, classification accuracy. This research question therefore remains unanswered until more studies are run, but the data suggests that certain PIN patterns might be harder to classify than others.

Overall three of the four research questions were sufficiently answered. The answers indicate that although adding pressure to the classification leads to significant improvement, the real life parameters of elapsed time and typing ability will need to be factored into the biometrics' development. However, the weak results on the effect of PIN design imply that classification accuracy can be improved by judicious selection of PINs.

The next chapter moves into the next phase of this dissertation that is, investigating the second research question, which focuses on the deployment of the keypad biometric technology. The first investigation measuring the potential for successful deployment addresses the purchase decision makers. Studies of what impacts their attitudes towards adoption are addressed in Chapters 7 and 8.

CHAPTER 7

RESEARCH METHODOLOGY-RQ2: EXECUTIVE INTERVIEWS

7.1 Introduction

The next four chapters investigate the critical factors that are necessary for successful adoption of new technologies. This chapter starts with a justification of why a triangulation of methodologies was used to investigate the critical factors necessary for acceptance of new biometric technologies. Details of the design and development of various interviewing instruments are then given followed by the procedures used to conduct the executive interviews. Lastly the chapter explains how various reliability and validity concerns were addressed.

7.2 Choice of Research Methodology for RQ2

Several data collection methods were considered with the two final candidate methods being the interview and survey method. Each of these two methods had certain advantages that were considered important for this study.

Rosenthal and Rosnow (1991) compare and contrast the interview and the survey methods. The interview method provides an opportunity to explore a new research area, where not enough is known for developing more precise methods as well as an opportunity to establish rapport with the subject and stimulate the trust and cooperation often needed to probe sensitive areas. Further the method provides an opportunity for the interviewer to help the subjects with their interpretation of the questions and allows flexibility in determining the wording and sequence of questions. Lastly the method

offers opportunity for getting new insights from subjects and probing on emergent issues which is vital at the exploratory stage. However it is time intensive and costly.

The survey method on the other had is easy to administer to large groups , is less costly in terms of resources (time and money) and can provide a higher degree of anonymity/privacy for sensitive issues as there is no face-to-face encounter. Further the method is is structured in that the respondents can only choose from a given set of answers which gives a common yardstick which is vital for a confirmatory study. However the survey does not offer the interviewer a chance to probe emerging issues.

A decision was made to use the interview method at the exploratory stage and the survey method at the confirmatory stage.

Thus the investigation for research question two was carried out in two studies. The first study was an executive's interviews exploratory study. It involved interviewing executive decision makers representing their organization to elicit the critical factors that determine the acceptance of a new biometric. The second study was user survey. This was a confirmatory study. It involved a survey to assess user perceptions on biometric keyboard technology as instantiated by a biometric ATM. The goal of triangulation (using more than one method) was to get a richer input from different groups of users and different approaches as recommended in ISA-4 (Malhotra and Groover 1998).

The rest of the chapter gives detailed methodology for the executive interview study while Chapter 9 has the methodology for user attitude study.

7.3 Objectives for RQ2:Executive Interviews Study

The objectives of the executive study was to (1) identify critical factors in adoption of new technologies from a decision maker's view (2) elicit from decision makers any important factors missing from preliminary biometric acceptance model built from the literature (3) to have decision makers rank the list of compiled critical factors in order of importance and (4) to get executive opinion on biometric keyboards

7.4 Subjects for RQ2: Executive Interviews

Four executives were chosen by the principal investigator from known contacts. The grounded theory approach recommends that theoretical sampling be used instead of random sampling. In theoretical sampling, the focus is in getting theoretically useful cases that confirms, extends and sharpens the theoretical framework from as many aspects as possible (Glaser and Straus 1967). In this study, the focus was on getting subjects with wide range of experience in introduction of new technologies and wherever possible with experience in the biometric security industry.

The subjects who were interviewed had experience introducing new technologies in financial fraud transaction monitoring, biometrics, and academia and in biotechnology. Thus the goal of varied experience was attained. However, grounded theory also recommends that the process should continue until theoretical saturation point is reached after which there is only marginal improvement in the formulated framework. This would have required finding at least two or three cases in each category so that some of the cases could be used to confirm theory formulated from earlier cases. This was not

done due to limitation in resources. The investigator acknowledges that this is a limitation on the generalizability of the results.

7.5 Investigating Critical Adoption Factors

The executive study was done in an iterative and exploratory way. It was driven by the *grounded theory approach* as recommended in (Glaser and Straus 1967) and applied in (Björck 2001; Eger and Blackey 2004; Pandit 1996).

The study was done under the recommended steps which includes review of technical literature and Selection of cases, development of rigorous data collection protocols, interviewing, data ordering, analysis of first case, theoretical sampling, closure and comparison with the literature (Glaser and Straus 1967).

Each of the steps was evaluated against four research quality criteria namely construct validity, internal validity, external validity and reliability

7.6 Development of Rigorous Data Collection Protocol

Grounded theory approach recommends a triangulation of different data collection protocols to ensure that the resulting theory is well grounded. To attain this objective, three methods were combined in the executive interviews study in a style similar to that reported in (Eger and Blackey 2004). The methods involved the preliminary review of general technology adoption literature as reported in Chapter two, case study analysis of several cases appearing in the literature as reported in the next Chapter 7 on results from case studies and conducting of in-depth interviews with four executives conversant with acceptance of new technologies as reported in this chapter

7.7 Preliminary Review of Technical Literature

The relevant technical literature in adoption of new technologies had already been gathered and reviewed as explained in chapter two of this dissertation. Research question two, investigating critical factors that would determine the acceptance of new biometric products was defined and a roadmap to address the question suggested. These roadmaps involved interviewing executives on critical adoption factors and then surveying end users on acceptance issues.

7.8 Development and Validation of In-Depth-Interview Instruments

The interviewing instruments were developed iteratively. The principal investigator wrote the first draft and then subjected it to face validity to ensure that the measures appeared to be a reasonable way of extracting the critical acceptance factors. The instruments were then passed on to two faculty members who suggested several refinements. These refinements were incorporated and the instrument taken back to the two faculty members. The final instruments consisted of executives' instruction sheets, consent form, executive summary on the biometric keyboard, interview script and a demographics collection sheet.

7.8.1 Executive Instructions Sheet

This document was given out to the executives at the start of each interview. It gave a break down of the tasks to be conducted in the interview which included the reading of the executive summary on biometric keyboard, signing the consent form, the actual interview and demographic data collection.

Please find the full executives instruction sheet in appendix F.

7.8.2 Executives Biometric Keyboard Summary

This consisted of a background to the development of the biometric keyboard prototype to mitigate identity fraud at the human computer interface. A request for an interview to discuss critical adoption factors that would determine the adoption of new technologies and opinion on biometric keyboard was then presented.

A detailed background of the extent of identity fraud was given and possible consequences of not controlling identity fraud given.

The principal investigator summarized progress made in developing a biometric prototype to mitigate identity fraud. A request was then be made for an interview appointment.

Please find the full executives summary sheet in appendix I.

7.8.3 Executives Interview Script

The executive's interview script was the main script guiding the interview. It had the interviews script and was used to by the researcher to ensure consistency in the quality of questions asked and thus avoided confounding measurement errors.

The interviewees were asked to give their background. A background to the identity fraud study was then given. This was followed by a request to get insights from the executive on the process of introducing new technologies like the biometric keyboard.

Once the interviewees agreed, a road map of the interview process was given so that the interviewee had an idea of the expected questions and time frame. The researcher would then follow the main questions on the interview script.

7.8.4 Executives Demographic Question Sheet

As the name suggests, this was the form used to collect demographic data from the executives. Data collected included age, gender, experience, education and an adopter category classification.

7.9 Interviewing Procedures

The interview procedure consisted of several steps. The interviews started with an introduction of the principal investigator to the interviewee. A background of the development of a biometric keyboard prototype to mitigate identity fraud was then given and some of the positive identification results described. A need to consider the business feasibility of the prototype was presented and the reason for approaching the interviewee for his/her insights on adoption of new technologies was given. This was followed by a roadmap of the interview and the expected time frame. The interviewee was asked to give a summary of their previous experience in introducing new technologies. The next steps were a request for the interview to consider the success and failure adoption and suggest factors that would have contributed to this outcome.

The preliminary biometric model was presented and explained as a formulation of existing literature case studies. The interviewee was asked to comment on the model and suggest additional factors or modifications. The next step was for the interviewee to rank

the innovation factors shown on the model in order of importance and to give justification for their ranking decision.

A detailed description of the biometric keyboard was given and the interviewee was then asked for their opinion on the prototype and then compares the biometric keyboard with other biometrics. The strengths and weaknesses of the biometric would then be considered.

7.10 Summary

The chapter started by justifying the use of more than one research methodology (triangulation) to answer the same research question. Two methodologies were chosen; the interview method given in this chapter and the user survey method given in Chapter 9. Details of the design and development of various interviewing instruments are then given followed by the procedures used to conduct the executive interviews. Lastly the chapter explains how various reliability and validity concerns were addressed. The findings from the interviews are given in the next chapter.

CHAPTER 8

RESULTS FOR RQ2 -EXECUTIVE INTERVIEWS

8.1 Introduction

This chapter gives the process used to code data from the executive interviews and the outcomes of the interviews. Several critical factors in the adoption process were suggested and ranked by the executive. Executive's opinion on the strengths of biometric keyboard technology and the issues that need to be addressed to improve the prototypes are then presented. Finally a final biometric acceptance model and six hypotheses showing the relationships of the identified factors are proposed.

The recommended steps in a grounded theory approach were given Chapter 7. The details of the first three steps (review of technical literature to interviewing) were reported in the methodology section of Chapter 7 so this chapter will report the remaining five steps and the findings.

8.2 Analysis of Previous Case Studies

The initial case in this study was the technical literature as recommended by (Glaser and Straus 1967) and applied by (Pandit 1996). Two case studies from the literature were studied to help identify factors which are important in adoption of new technologies.

The first case was a dissertation that investigated the factors that influenced information technology innovation diffusion (spread of usage) and infusion (depth of usage) at a sample of academic heath centers through surveying 1335 from 67 organizations (Ash 1997). Several factors were extracted from literature review and then

sorted out into three main categories. The first category had innovation attribute factors i.e. the characteristics of an innovation that either hinder or help the adoption and subsequent use of an innovation. The second set consisted of organizational attributes factors. These were the characteristics of an organization which either help or hinder the diffusion and use of an innovation. The third set of factors referred to as boundary-spanning attributes were the characteristics of the innovation –work interface and those who transfer information to and from information technology implementers and information technology users. Innovation attributes were found to be good predictors for diffusion and infusion except for infusion of CPR (Computer-based Patient Record) system. Organizational attributes were found to be good predictor for diffusion of CPR while boundary-spanning attributes influence the diffusion of email system.

The second case study investigated the factors that affected the adoption and diffusion of innovation in publishing and librarianships (Eger and Blackey 2004). The interviewee reported the innovation as the nucleus of the adoption and diffusion paradigm with quality emerging as the most important. The environment made up of threats and opportunities and was determined to be the second most important factor in adoption and diffusion. The were also concern the strategy that the supplier need to choose in developing the innovation, getting it into the distribution channel and informing and educating the market (Kotler 2003). Other issues raised included characteristics of the organization taking up the new innovation, characteristic of the people taking up the new innovation and the decision process that an adopter goes through from the time they hear of the innovation to the time they adopt (Rogers 1995).

8.3 Formulation of Preliminary Biometric Adoption Model

The formulation of the preliminary biometric model was done iteratively as suggested by grounded theory (Glaser and Straus 1967). The first step was to synthesize the case studies given in the previous section and the literature review. The two case studies above and the previous work that was done in the literature review section Chapter 2, Section 2.12 and 2.13 revealed several similarities in the models of adoption. The second and more challenging part of this investigation was to untangle the factors that are important for adoption from those factors that are important for user acceptance.

The executives in the end user organizations had to make decisions on what technology to purchase and adopt. However the successful adoption of any new technology is also dependent on its being accepted by the user. Thus the executives have to consider two sets of factors. The first set of factors concern adoption while the second set concern user acceptance factors. A look at the above case studies and previous literature gives some insight on this aspect. The review of user acceptance literature in section 2.12 suggested some of the important acceptance factors as performance expectancy, ease of use, facilitating conditions, social influence (Venkatesh et al. 2003). Chapter 2, Section 2.13 and the above two case studies suggested important adoption factors to be organizational factors , marketing factors, user differences and innovation attributes (Ash 1997; Rogers 1995). Comparing these two groups, the issues concerning the characteristics of the innovation are common to both groups. This were then viewed as the user acceptance issues while the unmatched factors that appears in adoption literature but does not appear in the user acceptance factors were grouped as adoption factors.

Two other factors were added in the second iteration from the interviews. The factor of cost was added as an adoption factor after being mentioned severally in the interview. Like wise the factor of trust –privacy issues was added in the second iteration as a user acceptance factor. This is because it was mentioned several times and on further investigation was also found to exist the in the literature (Cavoukian 1999; Gefen et al. 2003). A preliminary biometric model was formulated to help frame the findings made from above analysis. The model contained both user acceptance factors as well as user adoption. The acceptance factors included in the model were performance expectancy, ease of use, facilitating conditions (market timing), social influence and trust-privacy issues.

A preliminary model having these factors was formulated as shown below. This model was then taken to the executives for verification and extension.

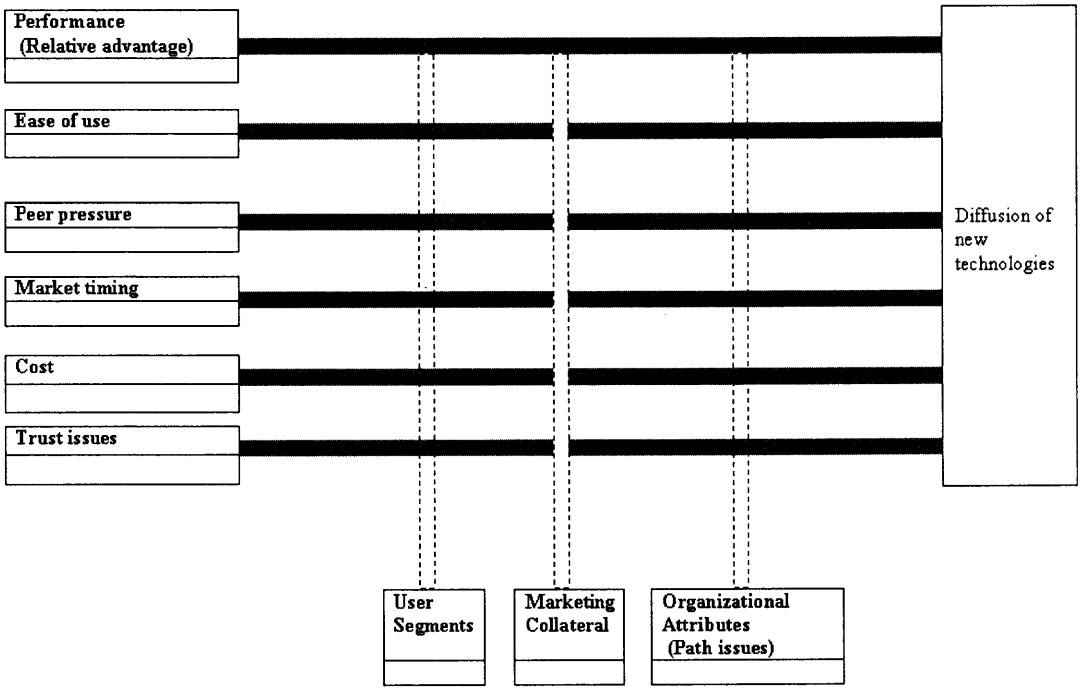

Figure 8.1 Preliminary biometric adoption model

8.4 Selection and Interviewing of Executives

Having extracted the above results from previous case studies in the literature, the next step as recommended in the grounded theory approach was to interview actual subjects as the next group of case studies.

Four executives were interviewed on adoption of new technologies. The first executive had over twenty years experience in introduction of new electronic memory products at a major Silicon Valley company, in introduction of fraud detection software in several of the leading banks and in design of biometrics identifiers in a leading academic research. The second executive was a generalist with over eighty years experience in introduction of new pervasive devices like the mobile phones, digital camera, notebook and digital organizers. The third executive had over forty five years of

experience with introduction of baby toys and also as the vice president of product development in a small software company. The fourth executive over twenty five years experience in introduction of new biotechnology and in nanotechnology in drugs discovery, delivery and diagnostics.

Two of the executives were male while the other two were female. Executive's selection was not random but rather based both on availability and potential to provide rich insights from previous experience in a certain area of interest.

8.5 Transcribing , Data Ordering and Coding of Executive Interviews

8.5.1 Transcribing

The principal investigator listened to the recorded interviews and transcribed the tapes into condensed transcripts. This involved listening to the tape one sentence at a time and summarizing the sentence into one or more main concepts.

8.5.2 Coding Scheme

A coding scheme was developed from the main categories extracted from the preliminary biometric model. The main categories were innovation, user characteristics, marketing and organizational attributes. The innovation attributes were of major significant to this study hence this category was expanded further into performance, ease of use and peer pressure subcategories. *Cost* was added as an additional subcategory to the innovation attributes subcategories after constantly appearing in the executive interviews.

Table 8.1 Coding Scheme for Critical Factors

Critical factor main categories	Critical factors subcategories
Innovation attributes	Performance
	Ease of use
	Peer pressure
	Market timing
	Cost
	Facilitating conditions
User segments attributes	
Marketing collateral attributes	
Organizational attributes	

8.7.3 Coding and Data Ordering Procedure

The transcriptions from each of the four interviewees were then exported into Nvivo software as documents. Each relevant sentence of the condensed script was coded into one of the subcategories of the above factors.

The subcategories were then ordered into clusters with other subcategories belonging to the same main category. The process was repeated for all the interviewee scripts. The end result was a set of critical factors with hierarchies of subcategories as shown in the figure below.

8.6 Factors Suggested by Executives

There were numerous factors suggested by different executives. Each executive concentrated in one or two areas and brushed through other areas. Ideally, the investigator should have continued interviewing more executives until there were no more new contributions coming from the executives. This point is called theoretical

saturation (Glaser and Straus 1967). However due to resource limitations, the investigator only interviewed four executives. This is a limitation in the study to be kept in mind when analyzing the resulting factors from the interviews that follow.

The figure below gives a network diagram made from the qualitative coding software. It shows the main factors and their sub-factors

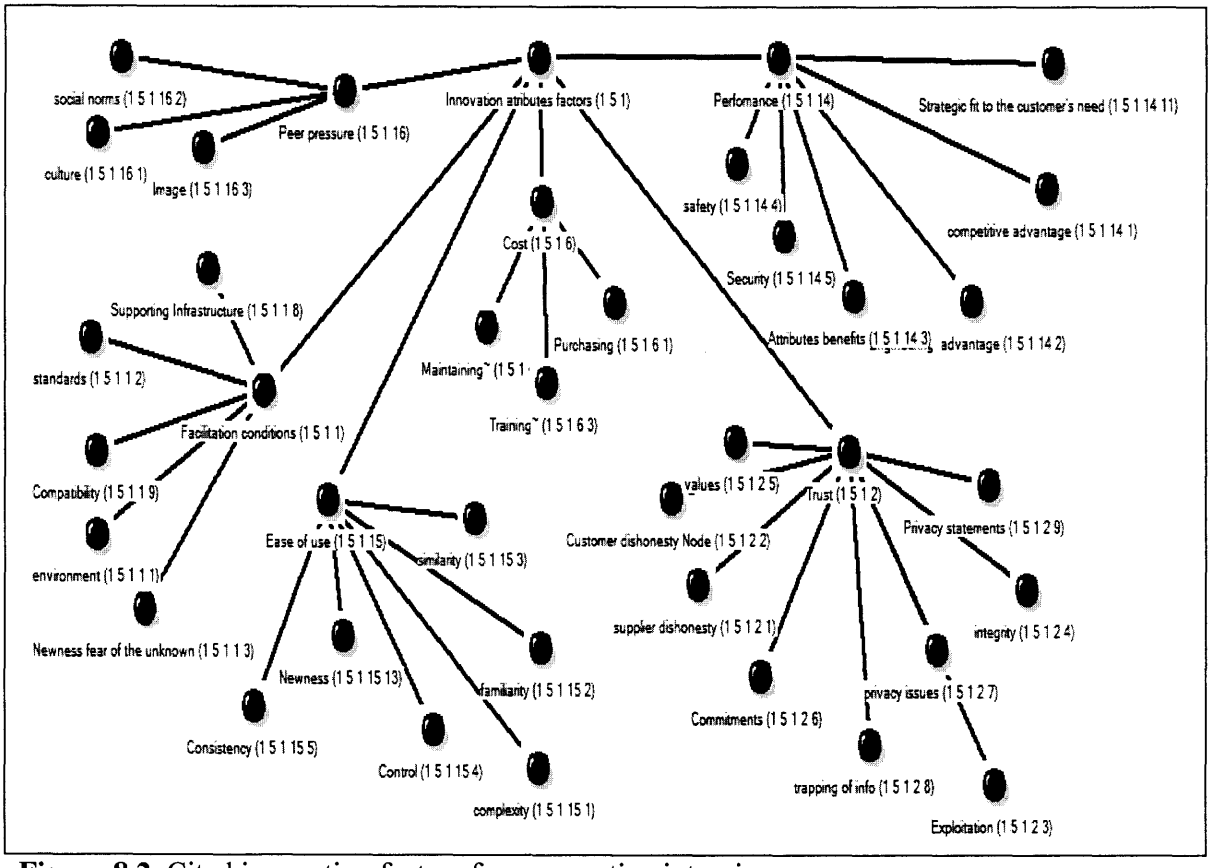

Figure 8.2 Cited innovation factors from executive interviews

8.7 Excerpts on Factors from Executive Interviews

The excerpts varied with different executives emphasizing different areas. However, most of the factors suggested by the executives fitted into one of the major critical factors categories from the coding scheme made earlier from previous literature. The holding categories were innovation attribute factors, user segment factors, marketing collateral attributes and organizational attribute factors. Below are excerpts from the interviews. The innovation factor categories had performance, ease of use, trust, peer pressure and facilitating conditions as subcategories. A cost subcategory was added after the first interview due to some remnants items that did not fit in the earlier main categories.

Table 8.2 Excerpts from the Interviews

Performance	"I think our product software failed not because our software was bad but because the hardware was unreliable" - Executive 1 "The customer will want to know the benefit of this product, its experiential advantage like increased reliability" - Executive 2
Ease-of-Use	"The whole idea of having to figure out a new interface puts me off - I keep postponing the decision to start using the interface even up to six months although it would probably just take an hour to learn the new interface" - Executive 2. "How easy is it to use the new technology without having to read the manual by using the general knowledge from use of previous systems?" - Executive2. "A system bound to failure will be a totally new interface , every thing totally opposite , no consistency , keyboard not like the regular QWERTY" -Executive2.
Peer Pressure	"The opener was black and sleek- every body wanted to have one to really feel that they belonged to the club"-Executive 3.
Trust-Privacy Issues	"In a couple of cases, pilot software was left in the client's premises and other start up companies reverse engineered the pilot software and came up with their own solutions similar to our product and started competing with us in other niches"- Executive 2. "I need to see the organization's privacy statement, on whether and how any trapped information is being used "- Executive 2.
Cost	"That product failed just because there was another cheaper clone computer executive 3 Our product cost are about 10-20 million dollars and it is going to take more than one year and a half before the institutions start seeing the benefits. It will require new computer systems which requires extraction of data from all the other systems and input to new systems and changes to the workflow systems"- Executive 1

Table 8.2 Excerpts from the Interviews (Continued)	
Facilitating Conditions	"The reason why I like the notebook is that it had the best features of the previous technology and the best features of the new technology. Most often, when they come up with new products, they get rid of the old one but this one had the best of both and that was why I like it - Executive 2. The reason why that computer was not buyable was because it was a disruptive innovation while the competition had standardized their computers – every body did things the same way and that way the competitors won"- Executive 3
User Segment Attributes	"The trick is to find early adopters – the trick is to find a set of customers in that market who have leadership; they understand and embrace new technological issues. It is also useful to find top tier institutions who are to act as references – select people who are braggarts- who will boast of how good your product is" - Executive 1
Marketing factors	"We failed because the competition was very hard"-executive 3 "We bundled our software with another company so as to succeed in penetrating the market"- executive 3 "We want products that are futuristic not me-too-products" - Executive 4
Organizational Factors	"A very important factor is to establish a team that is committed to success and success depend on partnerships gained" - Executive 4

8.8 Critical Factors Frequency Count from Interviews

The excerpts from the interviews give a qualitative idea of the important factors. However, there is a need to aggregate these factors in order to draw more inference. The table below shows a count of the factors given for each category.

Table 8.3 Frequency Count of Factors Cited in the Interviews

Critical factors generated from extant literature	Frequency of concept occurrence in interview with :				
	Executive 1	Executive 2	Executive 3	Executive 4	Total
Performance	3	5	2	9	19
Ease of use	2	15	1	1	19
Peer pressure			5	1	6
Trust-privacy issues	4	5	3	5	17
Cost (Added after interview)	2	6	3	1	12
Facilitating conditions/timing	3	2	5	4	14
Total Innovation attributes	14	33	18	21	85
User segments attributes	8	4			12
Marketing collateral attributes	14		3	8	22
Organizational attributes	9		1	18	28

It is observed that innovation attributes were the most frequently cited determinant of adoption of new technologies followed by organizational factors, marketing attributes and user segment attributes respectively. The innovation attributes most frequently cited were performance , ease of use and trust privacy issues in that order. The rest of this section will shed more light to innovation factors

The suggested factors and their frequency of occurrence can be used in deciding which aspects of a product should get higher attention. The category on innovation attributes occurred quite frequently which seems to imply that the category should get more attention. This is not to say that other factors like marketing and organizational management are not important.

8.9 Innovation Attributes Ranking by Executives

All the executives were asked to rank the five innovation attributes in the preliminary biometric adoption model in order of importance during the interview. The table below gives the ranking from each executive. The group rank is computed by summing the four ranking values given by the four executive for each attribute.

Table 8.4 Ranking of Innovation Attributes by Executives

	Executives					
Critical factors	No.1	No.2	No.3	No.4	Total	Group Rank
Performance	1	3	2	1	7	1
Ease of use	4	2	3	3	12	3
Peer pressure	3	5	5	5	18	5
Market timing	2	4	4	4	14	4
Trust issues	5	1	1	2	9	2

The factor that gets the highest group ranking by the executive interviews is performance of the innovation followed by trust issues, ease of use, market timing and peer pressure respectively.

This suggests that designers of biometrics should make sure that biometric innovation do achieve the required performance goals and should have the functionalities required to make sure that it does the job that it is designed to do. This will be the utmost test. The second most important attribute for the biometric should be that the biometric is not intrusive and does not invade user's privacy. Ease of use of the biometric will be the third factor to concentrate on.

8.10 Strength of the Biometric Keyboard as Cited by the Executives

The idea of a keyboard based method for mitigating identity fraud was explained to the executives. They were then requested to indicate the strong points that could be leveraged to make the innovation successful and also the issues that would need improvements for the keyboard biometric to be successfully adopted. The answers given were coded using the same coding scheme earlier generated for general for the critical factors. A hierarchy was made of all the suggested factors by clustering similar factors as per the coding scheme.

The figure below gives the strengths that came out of the interviews.

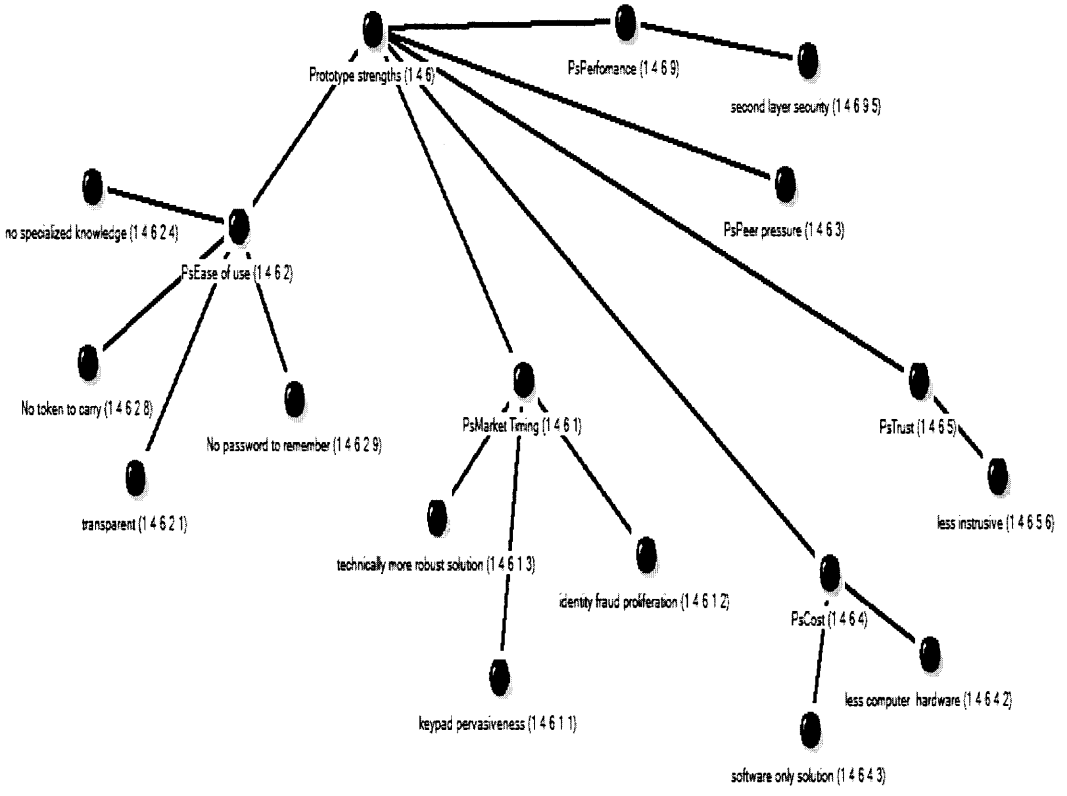

Figure 8.3 Biometric keyboard strengths from interviews

8.10.1 A Frequency Count of Biometric Strengths from Executive Interviews

Table 8.5 Frequency of Strengths Cited in Interviews

Critical factors	Executive one	Executive two	Executive three	Executive four	Total	Ranking
Performance	1	1			2	4
Ease of use	3	5		3	11	1
Peer pressure						6
Trust-privacy			1		1	5
Cost	3	3	3		9	2
Market timing	2	1			3	3

8.10.2 Biometric Keyboard Strengths –Excerpts from the Interviews

"The thing I like best about the biometric keyboard is that it can serve as a second authentication layer which is transparent"- Executive two

"The timing is now right for a biometric keyboard; identity fraud has proliferated to unprecedented levels" -Executive one

"Crime is now pervasive and every other person can relate to some personal or close persons losses" -Executive one

"The prototype does not require any extra effort and the user can just go on doing what they were using before" -Executive one

"The prototype is less intrusive and very little additional infrastructure is required " - Executive three.

The most frequently cited strength of the biometric keyboard was its ease of use followed by its cheap cost. Examples of such strength in the ease of use category were the biometric keyboards transparency, simplicity, easy revocability if password is compromised and previous experience of keyboard use.

8.11 Issues that could be Improved-Excerpts from the Interviews

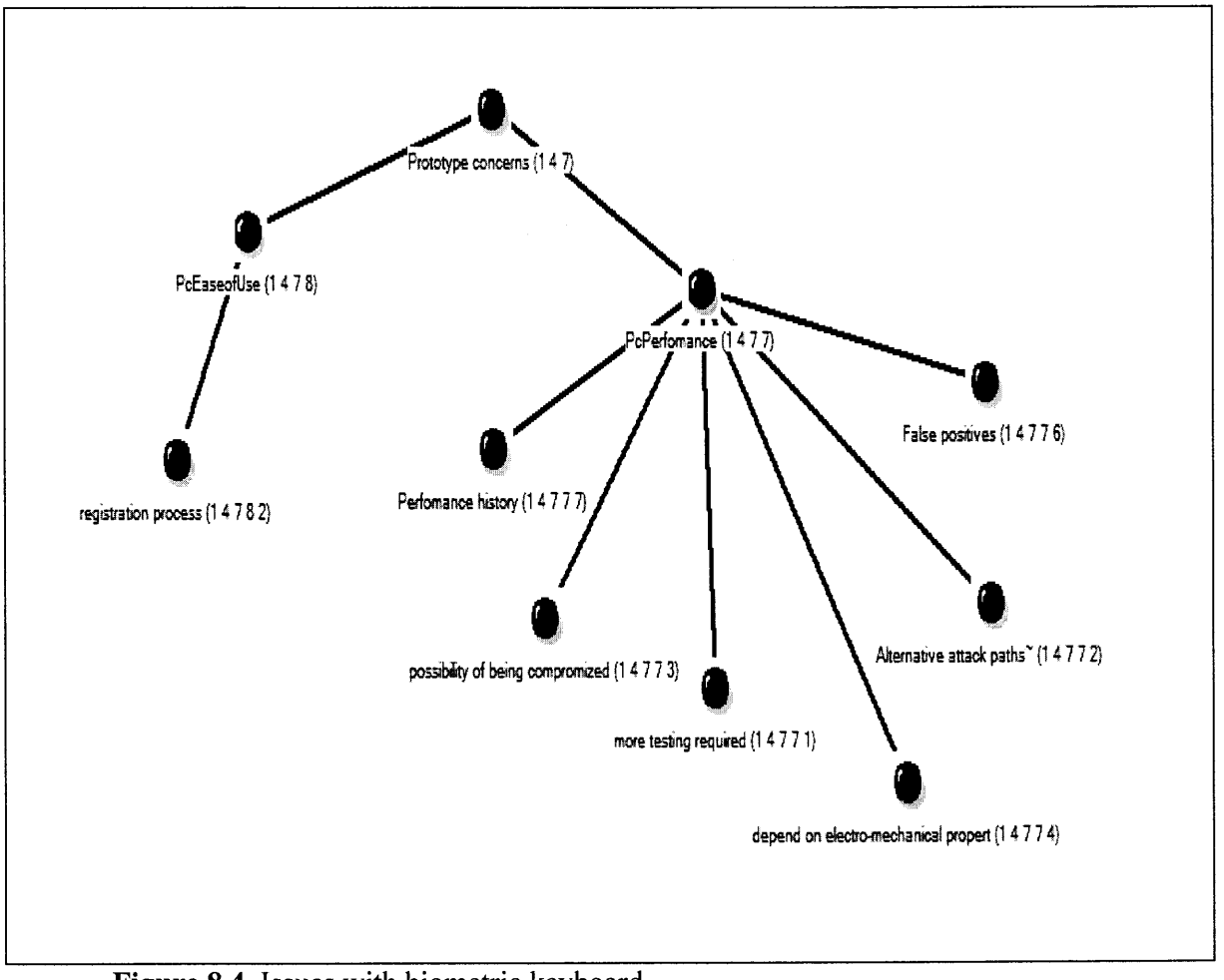

Figure 8.4 Issues with biometric keyboard

I think more testing is required to investigate the effect of different sensor pads on performance executive 1

Very little history is known about biometric keyboards executive two

The prototype depends on electro-mechanical properties which may vary with temperature, time or age executive 2

Why the keyboard path, while there are other possible entry paths like the mouse? executive 4

8.12 Frequency Count of Concern Factors Cited in the Executive Interviews

Table 8.6 Frequency Count of Concern Factors

Critical factors generated from extant literature	Frequency of concept occurrence with :				
	Executive-1	Executive-2	Executive-3	Executive-4	Total
Performance	4	3	9	2	18
Ease of use	2				2
Peer pressure					
Trust-privacy			1		1
Cost					
Market timing		2			2

It is observed that the most cited concern issue on the biometric keyboard was its performance

Several suggestions were given to improve the prototype. This include; (1) Making the registration process easier and less time consuming as possible, (2) Having a fall back plan in case some users could not use the method correctly , and (3) Doing further research to understand the effect of patterns aging on classification performance.

8.13 Generation of a Biometric Acceptance Model

The executive interviews gave insights which concerned the adoption of new technology. The first contribution of the interviews was a confirmation of the factors that had been suggested from the literature. The second contributions were the addition of trust-privacy factor as a user acceptance factor and the addition of cost as a managerial adoption factor to the biometric model. This was reviewed in section on formulation of preliminary biometric adoption mode. Executive managers make the decision of what technology to purchase and adopt. However the successful adoption of any new technology is also dependent on its being accepted by the user. Thus the executives have to adoption as

well as acceptance factors. To set a foundation of the next study which was a user survey, the research separated the factors of user acceptance from the factors of adoption.

The dissertation had earlier made a decision to extend the unified model (Venkatesh et al. 2003). The factors deemed important by the executives were compared with the factors in the unified model and the key factor that concerned user acceptance that came out of the interview seemed to be the trust-privacy issue. Cost factor was also new but it was deemed to be an adoption issues as it is the executives who have to justify the cost spend on any new technology.

The extension of the UTUAT model was done as follows:

The dependent variable was retained as behavioral intention to accept and use a new technology. The existing factors in the unified model were retained but redefined to apply to biometrics as detailed below.

Further the UTUAT was extended by addition of a Trust-privacy factor extracted from extracted from the interview but also covered by the literature (Cavoukian 1999; Gefen et al. 2003).

This resulted with an extended model with five constructs instead of the original four. The five constructs were redefined as follows.

8.13.1 Performance Expectancy Redefinition

This was redefined as the expectancy that a given biometric will offer a certain security advantage over other competing products which was operationalized as perceived security advantage. That it will offer this security advantages at all times and with the same certainty which was operationalized as systems reliability. That the biometric will

not be vulnerable to attacks from those who want access to the protected resource. This was operationalized as systems vulnerability. That the biometric will not falsely accept unauthorized users there by compromising the protected resource. This was operationalized as false acceptance rates.

8.13.2 Effort Expectancy Redefinition

This construct was redefined as the expectancy that a given biometric will be easy to use operationalized as perceived ease of use. That it will not reject the authorized user from accessing the protected resource. This was operationalized as false acceptance rate.
That it will respond within reasonable time to user request for authentication. This was operationalized as response time. That it will be easy to learn how to use and operate. This was operationalized as training time.

8.13.3 Social Influence Redefinition

This study retained the original definition in (Venkatesh 2000) of social influence as *the degree to which an individual perceives that important others believe (s)he should use the new system.* The construct was operationalized as subjective norms, social factors and image.

8.13.4 Facilitating Conditions Redefinition

This study retained the original definition in (Venkatesh 2000) of facilitating conditions as *the degree to which an individual believes that an organizational and technical*

infrastructure exists to support the use of the system. The construct was operationalized as market timing, user support, interoperability and standards.

8.13.5 Trust-Privacy Constructs Redefinition

This construct was redefined as the expectancy that a given biometric will faithfully protect the user from harm and offer guarantee to this. This was operationalized as trust. That the biometric will offer privacy to the user data stored for operations purpose. This was operationalized as privacy of user data. That the biometric will not be intrusive. This was operationalized as systems intrusiveness.

The final model is shown below with the two extra construct to the unified model slightly shaded in light blue.

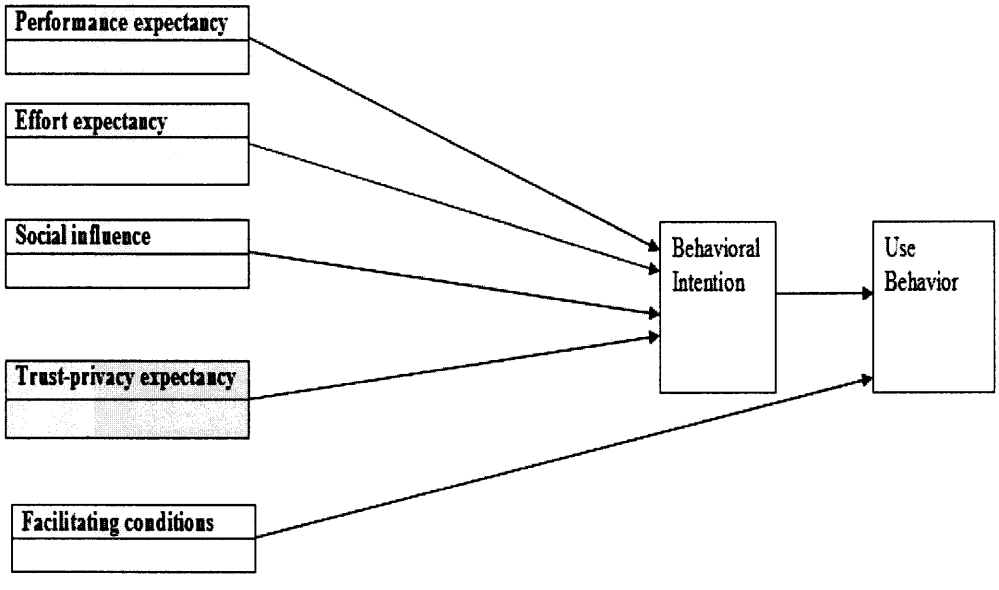

Figure 8.5 Biometric acceptance model

8.14 Formulation of RQ2 Hypotheses

The refined model implied that there will be five critical factors in acceptance of biometric keyboard technology. These factors are performance expectancy, social influence, facilitating conditions, trust-privacy and effort expectancy. The next step was to define the relationships between this critical factors and the dependent variable which was behavioral intention to accept and use new biometric technologies.

This dissertation proposes that the behavioral intention to accept and use keyboard-based authentication technology will be governed by the following hypothesis.

There will be a positive correlation between behavioral intention to use

and

H2a: Performance expectancy.

H2b: Social influence.

H2c: Facilitating conditions.

H2d: Trust privacy expectancy.

There will be a negative correlation between behavioral intention to use

and

H2e: Effort expectancy.

8.15 How Validity and Reliability Concerns were Addressed

Each of the steps given in the grounded theory approach was evaluated against four research quality criteria namely construct validity, internal validity, external validity and reliability.

Construct validity is enhanced by establishing clearly specified operational procedures (Pandit 1996) In this study , construct validity was enhanced by: (1) Conducting all interviews using the same set of clearly defined scripts and procedures. Thus all questions were framed from the same script hence the given answers were comparable since they were addressing the same questions. (2) Transcribing all the interviews to provide a standard document which the investigator used for coding. (3) Conducting all the coding using a standard coding scheme as given in the next chapter. (4) Building the theory and the skeleton of the preliminary biometric model from previous work to leverage on causal relationships earlier validated in given case studies. (5) Clearly defining and operationalizing all the variables.

8.16 Summary

The executive interviews study set out to investigate the critical factors that are important for successful adoption. Several sub-questions were suggested and the results discussed to address these questions. Research sub-question 12 sought to investigate the important critical factors. The ranking of factors suggested by executes given in this chapter suggested that the most important factors were performance, ease of use and trust-privacy issues. Research sub-question 13 sought to investigate the opinion of the executives on the factors that would positively or negatively impact the adoption of the keypad biometric. High ease of use and low cost were the most mentioned factors on the positive side while performance needed improvement. Research sub-question 14 sought to investigate any new factors that were not captured in the preliminary biometric adoption

model. This came out as cost by the second iteration. The table below concludes these results.

Table 8.7 Answers to Research Sub-Questions 12-14

No.	Research sub-question	Answer	Source	
12	What critical acceptance factors do executives believe will impact end user acceptance of a keypad biometric?	Executives believe performance, ease of use and trust and privacy will be the major factors.	Lit Review	Chapter 8 – results from interview
13	To what extent will the critical adoption factors presented in the research literature impact adoption for a keypad biometric?	The key adoption factors are perceived end user acceptance of the technology, cost and performance	Lit Review	Chapter 8 – results from interview
14	What, if any, new factors will affect executive adoption of the keypad biometric?	Cost was the primary new factor that came up		Chapter 8 – results from interview

Finally a final biometric acceptance model and five hypotheses showing the relationships of the identified factors were proposed.

CHAPTER 9

RESEARCH METHODOLOGY RQ2: USER ATTITUDES SURVEY

9.1 Introduction

The previous chapter formulated a biometric user acceptance model. This chapter extends the finding made from the executive interviews. The chapter gives the details on the development of a measurement instrument for the user attitude survey. A description of the subjects who participated is then given followed by steps that were taken to address various issues of validity.

9.2 Objectives for RQ2: User Attitudes Survey

The objectives of the user altitude survey were to measure user perception of biometric keyboard technology, validate the biometric acceptance model formulated earlier and investigate acceptable parameters for biometric keyboards.

9.3 Development of Survey Questionnaire

The questionnaire was developed in iterative phases as recommended by (Churchill 1979; Malhotra and Groover 1998) and applied in (Mohtadi 1998; Templeton et al. 2002).

The development phases were; (1) conceptual specification and definition of constructs, (2) construction of items, (3) data collection, and (4) measurement purification.

The first two steps will be reported in this chapter under methodology while the next two phases of data collection and measurement purification will be given in Chapter 10

9.3.1 Conceptual Specification and Definition of Constructs

The dependent variable (behavioral intention to accept and use new biometric technology) was hypothesized to depend on five independent variable constructs namely performance expectancy, effort expectancy, trust-privacy construct, social influence, and facilitation conditions.

A review of previous work in technology acceptance was done in chapter two. This was followed by an exploratory study in Chapter 8 and 9. The findings were synthesized into a biometric acceptance model given in the last chapter. These two research streams established the foundations for domain specification and redefinition of constructs as detailed in Chapter 8 (Formulation of biometric acceptance model). The redefinition of constructs produced determinants of the main five independent variable constructs given above.

The determinants of performance expectancy were operationalized as perceived security advantage, reliability, systems vulnerability and false acceptance rates. Determinant of effort expectancy were perceived ease of use, false rejection rates, response speed and training time. Trust-privacy construct was determined by trust, privacy of use data and systems intrusiveness. Facilitating conditions was determined by market timing, user support, interoperability and standards. Social influence was determined by subjective norms, social factors and image while cost construct was determined by purchase costs, training costs, maintenance costs, and usage fee expenses.

9.3.2 Construction of Items

The original draft of questionnaire included a total of 65 question items. The question items were generated from the determinants given above in the definition and conceptualization of constructs. However measurement scales for behavioral intention and social influence were adapted from those used in (Moore and Benbasat 1996; Venkatesh 2000).

Each question item was designed on a five-point likert scale. Responses ranged from strongly agree to strongly disagree.

9.4 Validity and Reliability Concerns in Questionnaire Development

Issues of validity and reliability were addressed by evaluating the questionnaire items against the ideal survey attributes yardstick reproduced below from (Malhotra and Groover 1998). This is an *authoritative best practice in survey research practice guide* used in information systems and marketing to give guidance on how question items should be designed. Care was taken to satisfy reliability and validity concerns in each phase as follows:

9.4.1 Steps Taken to Avoid General Errors

The unit of analysis was established as individual automated teller machine (ATM) users as representatives of themselves. This contrasted with the executive interviews described earlier in which the unit of analysis was the executive decision maker as a representative of the organization.

Table 9.1 Ideal survey attributes-Adopted from (Malhotra and Groover 1998)

General ISA-1. Is the unit of analysis clearly defined for the study? ISA-2. Does the instrumentation consistently reflect that unit of analysis? ISA-3. Is the respondent(s) chosen appropriate for the research question? ISA-4. Is any form of triangulation used to cross validate results?
Measurement error ISA- 5. Are multi-item variables used? ISA- 6. Is content validity assessed? ISA-7. Is field-based pre-testing of measures performed? ISA-8. Is reliability assessed? ISA-9. Is construct validity assessed? ISA-10. Is pilot data used for purifying measures or are existing validated measures adapted? ISA-11. Are confirmatory methods used?
Sampling error ISA-12. Is the sample frame defined and justified? ISA-13. Is random sampling used from the sample frame? ISA-14. Is the response rate over 20%? ISA- 15. Is non-response bias estimated?
Internal validity ISA-16. Are attempts made to establish internal validity of the findings?
Statistical conclusion error ISA-17. Is there sufficient statistical power to reduce statistical conclusion error?

All question items were refined to directly address the individual thus satisfying ISA-1(unit of analysis clearly defined) & ISA-2(all items to consistently reflect the unit of analysis). Two question items concerning the determinants of the cost construct (device cost and maintenance) and one determinant of facilitating condition construct (compatibility and standards) were dropped as the target audience was deemed unknowledgeable in such matters. ISA-4 (recommendation of triangulation) was met since research question two was investigated using two research methodology (user survey and executive interviewing).

9.4.2 Steps Taken to Avoid Measurement Errors

Measurement errors are one of the most common and significant sources of error in surveys (Malhotra and Groover 1998). Every effort was taken to avoid such errors as explained below.

9.4.2.1 Use of multi-item scales. ISA-5 recommends the use of multi-item measures to help balance off measurement errors that may be inherent in one question item. This study ensured that all constructs were measured using multiple items.

9.4.2.2 Content validation. ISA-6 recommends that content validation be undertaken to ensure the appropriateness of the question items. The first thing that was done was make a clear definition of the domain of each construct as explained early in chapter two (building the biometric acceptance model). Each construct was redefined and the determinant of each construct defined. The second step was the use of existing scales wherever possible. Thus the scales on behavioral intention to accept/use new technology and the scale on social influence were scales validated from previous studies. Likewise some items in the facilitating conditions and effort expectancy were also adapted from validated scaled although they were rephrased to address biometric ATM.

The principal investigator and a faculty well versed in question generation and validation then iteratively went through the questions refining and further removing questions that did not directly address the domain of each construct. By the fifth iteration, the questionnaire had 39 question items which were deemed important. These were retained for the next stage of validation by pre-testing.

9.4.2.3 Pre-testing. ISA-7 recommends that a field-based pre-testing of the measure be performed to identify question items issues that can lead to error. In pursuit of this goal, the questionnaire with thirty nine question items was then distributed to a group of seven researchers for pre-testing. The overriding goal was to select people with as much expertise (in questionnaire design/survey research) as possible with minimal costs in terms of time and resources.

The first researcher was a distinguished professor teaching research methodology courses at the doctoral level at a university in the east coast. The other six researchers were doctoral students in various stages of doctoral research. Each of them had done at least one research methodology course and most of them had done a major survey study either for their dissertation or for publication purpose. Each researcher was asked to respond to all the questionnaire items. In addition they were asked to make comments over question items that needed improvements. Such improvement included rewording, clarifying, simplifying etc. The principle investigator had a one-to -one post-questionnaire period with each of the researcher going through the question items with an emphasis on question items with researcher's comments or in which the answer chosen was unexpected. Further adjustments were made in fine-tuning the thirty nine question items. The refined questionnaire was then given to a researcher who recently defended and passed her doctoral dissertation which was wholly based on the survey methodology. The target was to catch any errors that may have been created during refining and also to preempt any post questionnaire issues that may arise in data analysis and model validation using the available structural modeling software (PLS). Finally the questionnaire was given to a nursing student in a community college in the east coast.

She was asked to complete the questionnaire and also mark question items which were difficult to understand or ambiguous. The goal for this was investigate where there are questions that would be difficult to an audience that had little computer exposure. Comments made by the nursing student were also acted upon and the questionnaire refined.

The final version of the questionnaire is given in the appendix M.

9.5 Measurement Scales for RQ2:User Survey

Measurement scales were developed to measure the constructs in above model. All constructs in the survey were measured using a 5 point Likert scale as follows.

Table 9.2 Measurement Scale for Performance Expectancy

Determinants	Question statements	Source
False acceptance rates	Q20- I believe that a biometric ATM will be more likely to prevent thieves from using my ATM card than a standard ATM. Q25- I believe that it will be harder for thieves to trick a biometric ATM Q31 - Current ATM systems are secure enough without biometrics	New
Systems vulnerability	Q23-I worry that someone could steal my personal identity from a biometric ATM Q5-I am concerned that someone could steal my typing patterns from a biometric ATM Q13-I am concerned that someone could copy my typing patterns from a biometric ATM and reuse them to steal money from my account	New
Reliability	Q33-I am concerned that I will have a bad day and the biometric ATM will not be able to recognize my typing patterns Q30-I worry that a biometric ATM that I don't normally use will not recognize my typing patterns	

Table 9.3 Measurement Scale for Behavioral Intention

Question statements	Source
Q19- I would use a biometric ATM machine if it were conveniently located Q11- I would avoid using a biometric ATM. Q8- I intend to use biometric ATMs once they are installed	(Venkatesh 2000)

Table 9.4 Measurement Scale for Effort Expectancy

Determinants	Question statements	Source
Perceived ease of use	Q-9- I feel that interaction with a biometric ATM will be clear and understandable Q29-I feel that it will be easy to get the biometric ATM to execute the bank transactions that I usually need Q4-A biometric ATM will be too difficult to use	(Moore and Benbasat 1996)
False rejection rates	Q12-I am worried that a biometric ATM will not always recognize me as a valid user. Q26-I am sure that a biometric ATM will have no problems verifying me as the real user.	New
Response time	Q1- I am worried that a biometric ATM will take too long to verify my identity Q5-The identity verification on a biometric ATM will require repetition	New
Training time	Q10-I think my typing is so variable that it will be hard for me to learn to use a biometric ATM. Q7- I am concerned that the typing training required to use a biometric ATM will take too long.	New

Table 9.5 Measurement Scale for Trust-Privacy Construct

Determinants	Question statements	Source
Privacy of user data	Q2-I am concerned that the biometric typing patterns may be shared with other organizations without my consent. Q24-I am concerned that the collected biometric typing patterns may be used for other purpose like monitoring my activities without my consent	New
Systems intrusiveness	Q16-Capturing my biometric typing pattern is a serious invasion of my privacy. Q32-The biometric ATM system is an invasion of personal privacy. Q17-The biometric ATM process of authenticating a user as valid via typing patterns is degrading	New
Trust	Q15-I really don't believe banks are protecting me from identity fraud when they install the biometric ATMs. Q28-I fully believe that the sole reason the banks are introducing the biometric ATMs is for better protection of my money.	New

Table 9.6 Measurement Scale for Social Influence

Question statements	Source
Q18-If I was the first to get a biometric ATM account, I would impress my friends with this information. Q9-My friends will think that using a biometric ATM is cooling (wise).	(Venkatesh 2000)

Table 9.7 Measurement Scale for Facilitating Conditions

Determinants	Question statement	Source
Timing	Q21- Given the increasing cases of identity fraud, I feel that the time is right to start using the biometric ATMs	New
Facilitating conditions	Q27-My experience with computer keyboards and ATM keypads will make the switch to biometric ATMs easy. Q3-I believe that no special knowledge or skill is needed to use new biometric ATMs. Q22-I feel confident that I know how to type in consistent machine-acceptable biometric patterns	New

Several questions were designed to measure acceptable parameters for biometric keyboard as follows

Table 9.8 Measurement of Acceptable Biometric Keyboard Fee

Question statements					Source
Q34 I am willing to pay up to ($_____) for every biometric ATM use if it prevents someone from falsifying and using my card.					New
0	1	2	3	4	
$0.00	$0.10	$0.25	$0.50	$1.00	

Table 9.9 Measurement of Acceptable False Acceptance Rates

Question statements						Source
Q35-If you are at an ATM machine that uses a keystroke biometric security system and really need cash but are already late for work, how many times would you be willing to retype your PIN number if the machine had trouble verifying your PIN? (Circle the number, which best applies.)						New
	0	1	2	3	4	
	Zero more times	One more times	Two more times	Three more times	Greater than three times	
Q36-If you are at an ATM machine that uses a keystroke biometric security system on a day in which you have nothing scheduled, how many times would you be willing to retype in your PIN number if the machine had trouble verifying your PIN?						
	0	1	2	3	4	
	Zero more times	One more times	Two more times	Three more times	Greater than three times	

Table 9.10 Measurement of Willingness to Provide Training Samples

Question statements					Source
Q37-Imagine you are opening a new bank account. Please circle the number of times you would be willing to type in your PIN number in order for the biometric ATM to learn your unique typing pattern.					New
0 Five times	1 Ten times	2 Fifteen times	3 Twenty times	4 > Twenty times	
Q38-How many times in a year, would you be willing to re-train the biometric ATM to update your unique PIN number typing pattern?					
0 Zero time	1 One time	2 Two times	3 Three times	4 > Four times	
Q39-I do not mind going to my bank and repeatedly typing my PIN number for 10 minutes in order to create a unique biometric signature for my PIN number.					
0 Strongly Disagree	1 Disagree	2 Neutral	3 Agree	4 Strongly Agree	

9.6 Subjects for RQ2: User Attitudes Survey

ISA12-15 of the ideal survey attributes (Malhotra and Groover 1998) recommends that sampling errors can be avoided by properly defining the sampling frame , randomly sampling the subjects and taking steps to improve the response rate beyond the minimum 20%.

The true target population of the survey was defined as all current/potential users of bank ATMs. However, due to time and resource constraints, the final sample was drawn from university students. Students are among the most frequent users of ATM systems but the study cannot claim that this sample was fully representative of the true population. Seven classes of computing undergraduate students in a university in the east coast were initially contacted for participation. Later another group of nursing undergraduate majors was contacted to have a more balanced population. Efforts to boost response rates included follow-ups on several cases and a standing offer of 3% extra credit on final semester grade to majority of classes.

9.7 Survey Procedures for RQ2: User Attitudes Survey

The subjects were given a diagram showing the new Biometric ATM followed by a description of the attributes and operations of the new biometric ATM given below. The goal was to have a mental instantiation of the biometric keyboard in the subject's minds

9.7.1 Biometric Scenario

Figure 9.1 Instantiation of biometric ATM scenario

9.7.2 Description of Biometric ATM

The information systems department at NJIT is working on new technology that will sense the pressure and time patterns exhibited by a user when typing their personal identification number (PIN). This use of unique behavior patterns to identify a person is called a biometric measure. The first application of this biometric technology will be on ATM machines. We will replace the current ATM keypads with new keypads that can detect a person's typing pressure and time patterns. However the new keypads will look and feel exactly like the existing keypads. Likewise the current ATM procedures will be the same. The only difference will be that the user typing pressure and time patterns will be captured and used along with the PIN to verify that the user is indeed the genuine user and not an imposter. This new ATM with biometric technology will hereafter be referred to as the BIOMETRIC ATM'

9.7.3 Survey Task

The subjects were then asked to fill in a consent form followed by survey questionnaire. Both are shown in the Appendix K

9.8 Summary

The above chapter gives the development of various measurement scales for the user attitude survey and the steps that were taken to ensure reliability and validity. The results of user survey as given in the following chapter.

CHAPTER 10

RESULTS FOR RESEARCH QUESTION 2: USER ATTITUDE SURVEY

10.1 Introduction

This chapter gives results from the user attitude survey starting from descriptive statistics, validation of biometric acceptance model and variables that were found to have a mediating effect on the model.

10.2 Objectives

The objectives of the user altitude survey were to measure user perception of biometric keyboard technology, validate the biometric acceptance model formulated earlier and investigate acceptable parameters for biometric keyboards.

The design and preliminary validation of the survey instrument was given in Chapter seven. Care was taken to satisfy validity and reliability issues to the best of the investigators ability as explained in chapter nine.

10.3 Demographic Characteristics of the Subjects

10.3.1 Response Rate

159 subjects successfully completed the questionnaire out of a total of 270 who were initially contacted. This gave a response rate of about 59 % which is above the required minimum of 20 % (Yu and Cooper 1983). An extra credit of 3% on the final semester grade was offered for most of the participating classes to encourage higher participation.

An analysis was made of those who did not respond and it was found that most of them had actually completed the survey in another class. Most students took about four classes any of which could have been among the contacted classes.

10.3.2 Gender

There were 47 females and 112 males in the study. This gives percentages of 29.6 % females and 70.4% males respectively.

Table 10.1 Gender Distribution			
Gender	Male	Female	Total
Number of subjects	112	47	159
Percentage	26.6%	70.4%	100%

This is close to the gender distribution in the general college population of the university where the students were drawn from.

10.3.3 Age

70 % of the subject population was between 18-25 years old.

Below is a table with full details.

Table 10.2 Age Distribution				
Age in years	18-25	26-33	34-41	>= 42 years
No. of subjects	110	26	14	9
Percentage	69.2%	16.3	8.8	5.7%

The above is reflective of the student population from which the sample was drawn.

10.4 Acceptable Guidelines for The Biometric ATM

Users were requested to indicate the acceptance guidelines on various aspects of the biometric ATM as follows;

10.4.1 Acceptable Biometric ATM Fee

Users were asked to indicate the maximum fee that they would be willing to pay per biometric ATM use if the later helped prevent fraud.

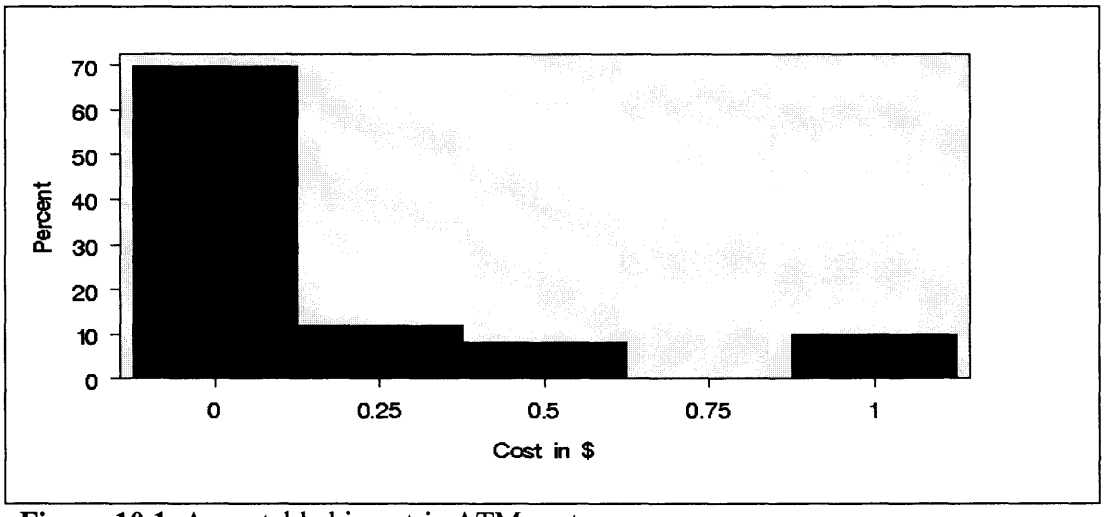

Figure 10.1 Acceptable biometric ATM cost

The distribution of acceptable cost per use is shown in the figure above. 70% of user population indicated that they were not ready to pay any money for biometric ATM even if the later could help prevent fraud. This shows that users are not ready to foot any cost for additional security. One possible explanation would be that users believe that the banks should meet cost of making the banking systems secure. Another possible explanation could be that the users do not believe that there is need for the biometric ATM.

10.4.2 Acceptable Number of Re-Types when in a Hurry

Users were asked to indicate the number of times that they would be willing to re-type their PIN if they were in a big hurry and badly needed cash. The answers ranged from zero to more than four times. The histogram below shows the distribution of the answers.

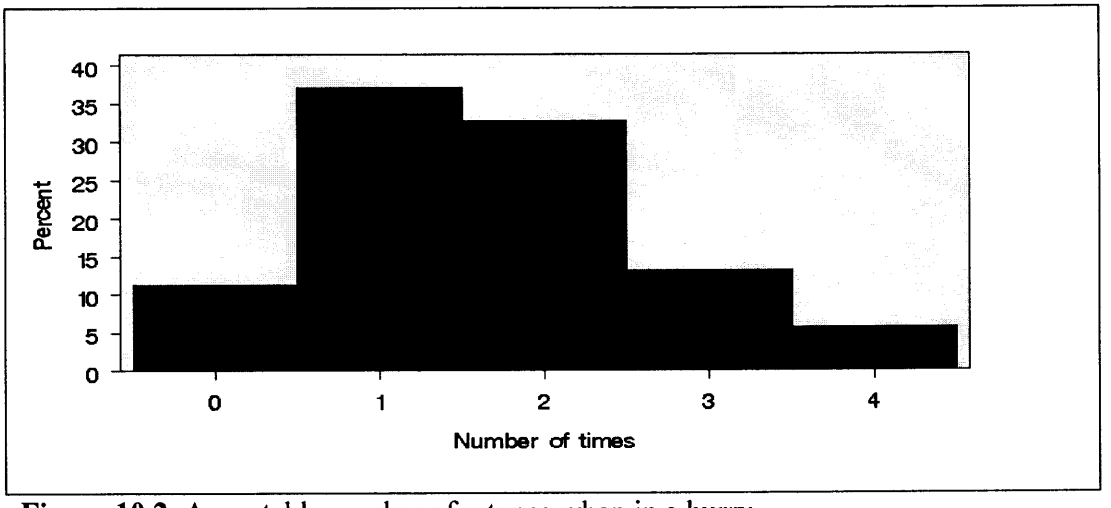

Figure 10.2 Acceptable number of retypes when in a hurry

It is observed that most of the users were ready to re-type once or twice if the biometric ATM had trouble verifying the user. The performance of a biometric is determined by the false acceptance and false rejection rates. Decreasing false acceptance rates increases false rejection rate. The implication of the above finding is that we can make it harder for intruders to fool the biometric ATM by reducing false acceptance rates up to the point where the user has to retype one or two times but not beyond this point.

10.4.3 Acceptable Number of Retype Times when Relaxed

Users were asked to indicate the number of times that they would be willing to retype their PIN if they had nothing scheduled. The answered ranged from zero to more than four times. The histogram below shows the distribution of the answers.

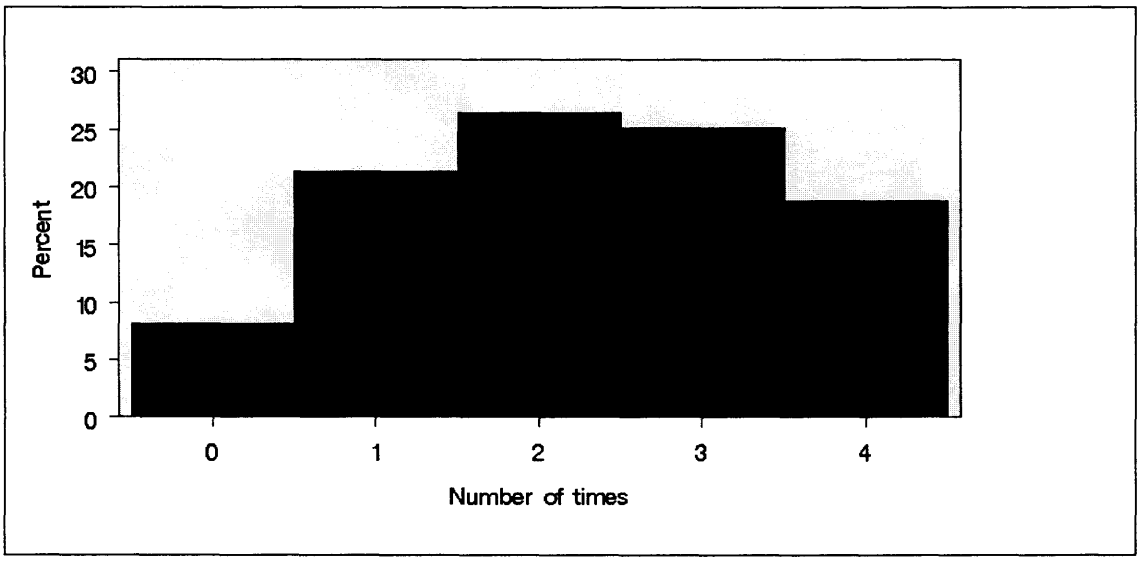

Figure 10.3 Acceptable number of retypes when relaxed

It is observed that users are willing to retype 2-3 times if the biometric ATM has trouble verifying the user. This gives more leeway but we may have to design for the user who is in a hurry to be sure of catering both groups' needs. Thus in practice the ATM will at most have to ask for two retypes and then go into a fall back mechanism.

10.4.4 Acceptable Number of Registration Patterns

Users were asked to indicate the number of times they would be willing to type their PIN during registration so as to provide the biometric ATM with samples for later verification of the user.

It is observed that about 48 % of users want to type five times only while another 28 % would be willing to type up to 10 times. Beyond this point most of the users would not co-operate.

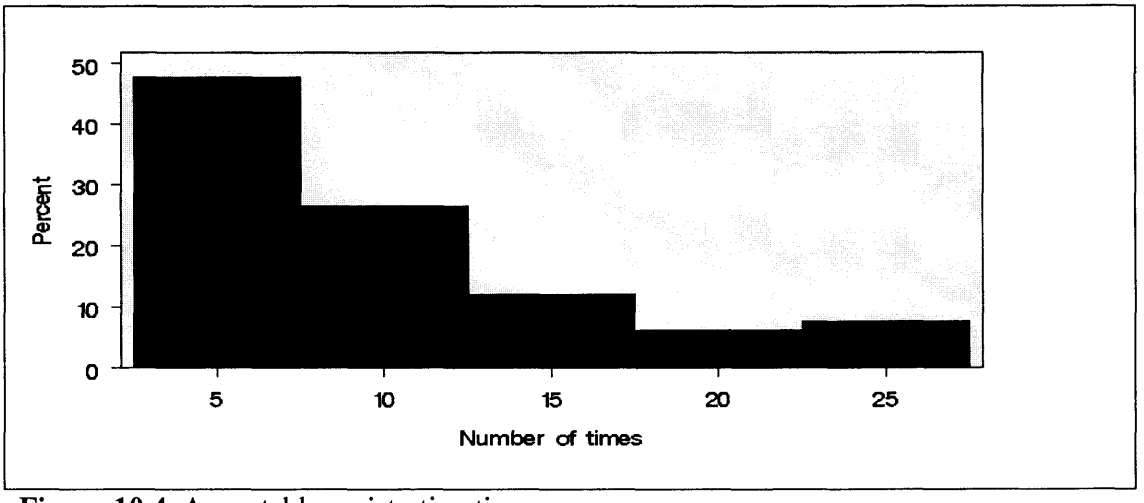

Figure 10.4 Acceptable registration times

10.4.5 Acceptable Retraining Times per Year

Users were asked to indicate the number of times per year that they would be willing to retrain the biometric ATM.

It is observed that over 80% of the users are only willing to retrain the biometric system a maximum of 2 times per year.

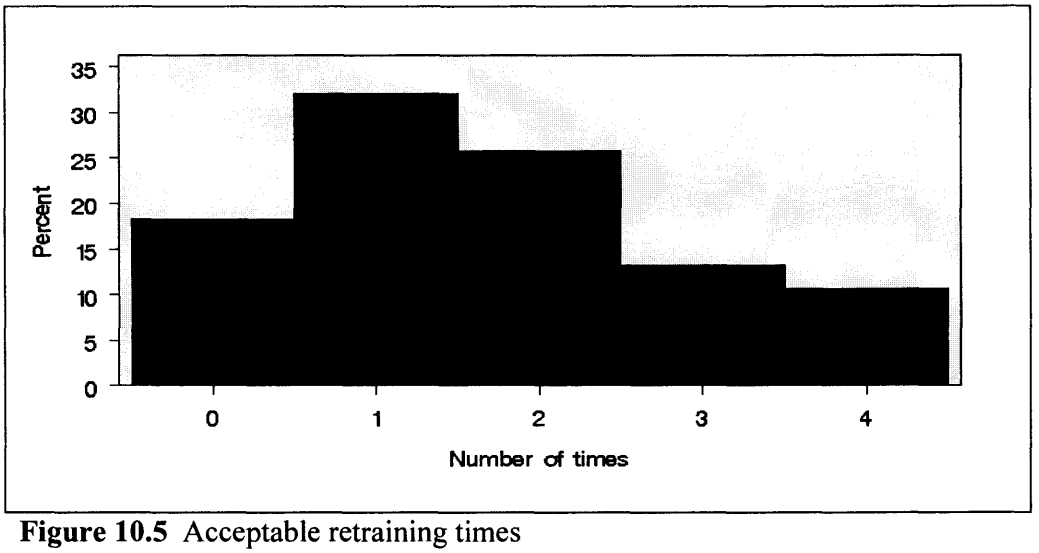

Figure 10.5 Acceptable retraining times

10.4.6 Acceptable Duration for Registration

Users were asked if they would be agree to sped 10 minutes repeatedly typing their PIN in order to create a unique biometric signature for the PIN number.

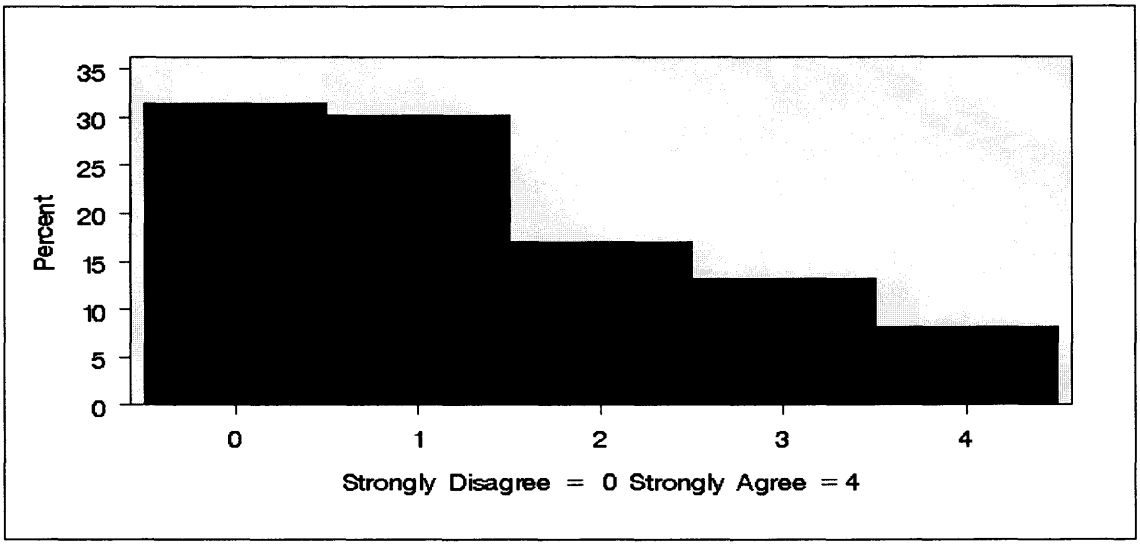

Figure 10.6 Acceptable duration for registration

It is observed that over 60% of the population would not agree to repeatedly type their PIN for ten minutes.

10.5 Descriptive Statistics and Tests for Normality

10.5.1 A Review of Test for Normality

The objective of normality test is to investigate whether the sample data is normally distributed. Parametric statistics assume that sample data is from a normal distribution hence it is prudent to confirm whether this assumption is true before performing parametric tests.

This study used several approaches to investigate normality. A histogram was made for all data distributions followed by a computation of the mean and standard deviations on the questions item scores so as to get a good grasp of the data descriptive statistics. Histograms were also made for the distribution to aid in visualization of the data distribution. The skewness and kurtosis of the data was then computed. The last test to be performed was a Wilk-Shapiro to confirm the visual observation on normality of data distributions. A brief review is given for an understanding of the performed test:

Wilk-Shapiro: This is the most popular test for normality (Conover 1999). The test work by setting the Hypothesis as follows

H0: Data is normally distributed

The null Hypothesis is rejected if the data p-value < 0.05 and an inference maybe that the data is not normal.

Kurtosis: This refers to the sharpness of the peak. Normal distributions should give a kurtosis =3

Skewness: This refers to the symmetry of the data distribution. Normal distributions should have a skewness =0. Negative values suggest that the data is heavier on the left tails and vice-versa for positive values.

Histograms: This gives a visual picture of how the data is distributed and should always be the starting point of normality test.

10.5.2 Data Preprocessing for Descriptive and Normality Analysis

All the question items were answered on a Likert scale of 1-5 with 5 being the best score. Negatively phrased question scores were reversed so that all the scores were in one

direction. Some constructs had more items than other constructs so the mean of each construct (divide total score on the construct items by the number of items) was computed so that they can be comparable with other constructs .Thus the mean item score for a construct like effort expectancy with eight question items was computed by dividing the sum of the scores got on the eight items dived by the number of items in the scale (=8). The next step was computation of the group mean score for all the respondents. Further, the standard deviation, Wilk-Shapiro statistics, kurtosis and skewness of all constructs was computed. Histograms were also made for all the constructs to aid in analysis.

10.5.3 Performance Expectancy Distribution and Test for Normality

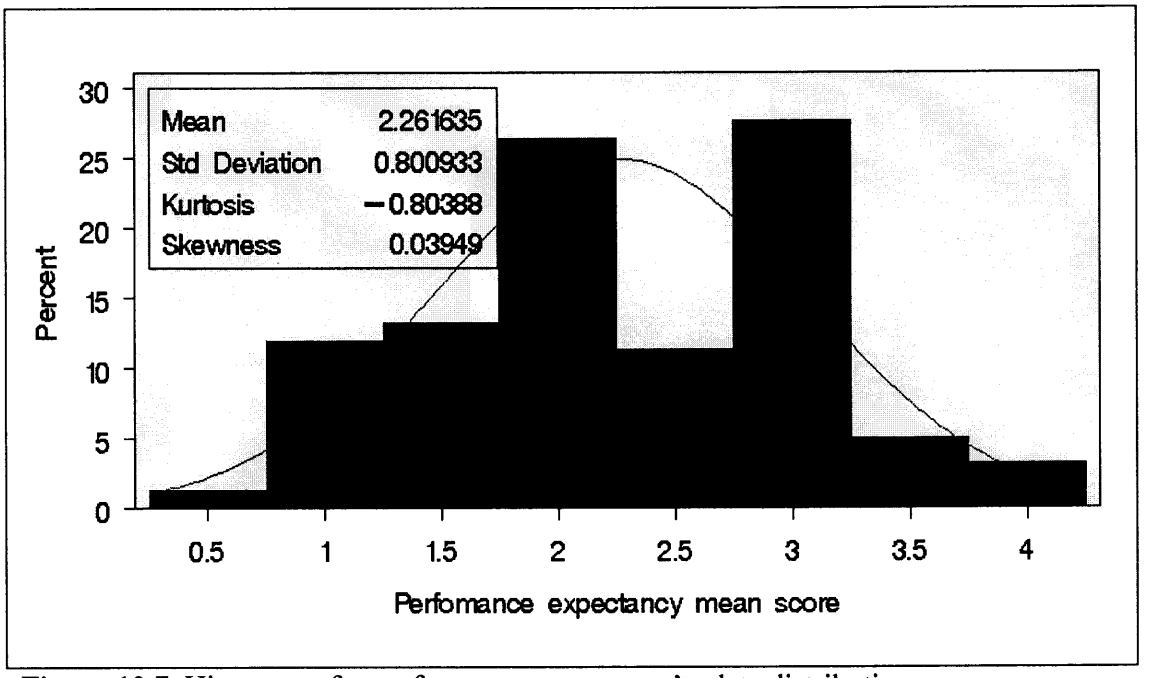

Figure 10.7 Histogram for performance expectancy's data distribution

.

The figure above shows a histogram of performance expectancy distribution while the shown curve is the ideal data curve if the data is normally distributed.

The mean item score for the performance construct is 2.26 on a scale of 5 and a standard deviation of 0.8. There are two clusters of users, those that rate the biometric ATM with a high performance with a mean item score of 3 and another cluster of users who are not so sure of the biometric keyboard performance with a mean item score of around 2. This would suggest that the group with lower perception of the performance of the biometric ATM has concerns that need to be addressed if the biometric ATM is to be introduced. Those with high perceptions of the biometric ATM could be used as the early adopters in order to show-case the technology so that critical number of users adopts the technology. A visual check at the histogram for normality test shows that the constructs data is not normally distributed as it deviates widely on some points from the fitted normality curve. This conclusion that the construct distribution is non-normal was confirmed by the tests given below. The Shapiro-Wilk test had a $p<0.0049$ hence the null Hypothesis was rejected. The conclusion was that the data is non-normal and non parametric tests were used for this construct.

Table 10.3 Normality Test for Performance Expectancy Data Distribution

Tests for Normality

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.974506	Pr < W	0.0049
Kolmogorov-Smirnov	D	0.111013	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.269374	Pr > W-Sq	<0.0050
Anderson-Darling	A-Sq	1.572088	Pr > A-Sq	<0.0050

10.5.4 Effort Expectancy Descriptive Statistics and Tests for Normality

The histogram below shows the data distribution for effort expectancy mean question items scores. The mean score of the whole group is 1.9 with a standard deviation of 0.58. There are two groups of users. One group with mean effort expectancy less or equal to 1.5 expects to put a very low effort in order to have the biometric ATM perform the expected functions. In other words, this group believes that the ATM is easy to use and would be the first group to target if ease of use is the major determinant. The second group of users with mean effort expectancy around 2.1-2.4 is neutral on the biometric ATM's effort expectancy. This is the undecided group and their concerns would need to be addressed if they are to become users of the biometric ATM.

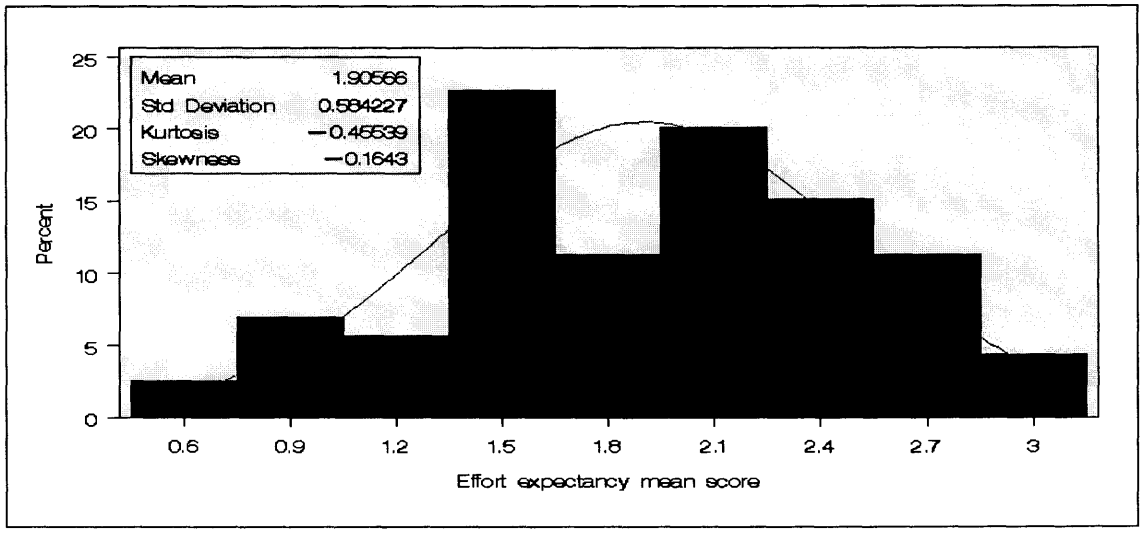

Figure 10.8 Histogram for effort expectancy data distribution

The above observation that the data is in two clusters also imply that the data is not normally distributed. The histogram bar heights are also seen to deviates from the ideal normal distribution curve shown enveloping the histogram.

Table 10.4 Normality Test Statistics for Effort Expectancy Construct

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.985466	Pr < W	0.0954
Kolmogorov-Smirnov	D	0.073575	Pr > D	0.0346
Cramer-von Mises	W-Sq	0.099692	Pr > W-Sq	0.1154
Anderson-Darling	A-Sq	0.620514	Pr > A-Sq	0.1054

The above shows the normality statistics for the effort expectancy construct. W=0.986 p=0.0954. Since p >0.05 then we cannot reject the null Hypothesis (H0 = data is normally distributed). This statistics are on the borderline. The study used the evidence of the skewness, kurtosis and the visual histogram to decide that the data was not normally distributed and non-parametric tests were used.

10.5.5 Trust-Privacy Descriptive Statistics and Normality Testing

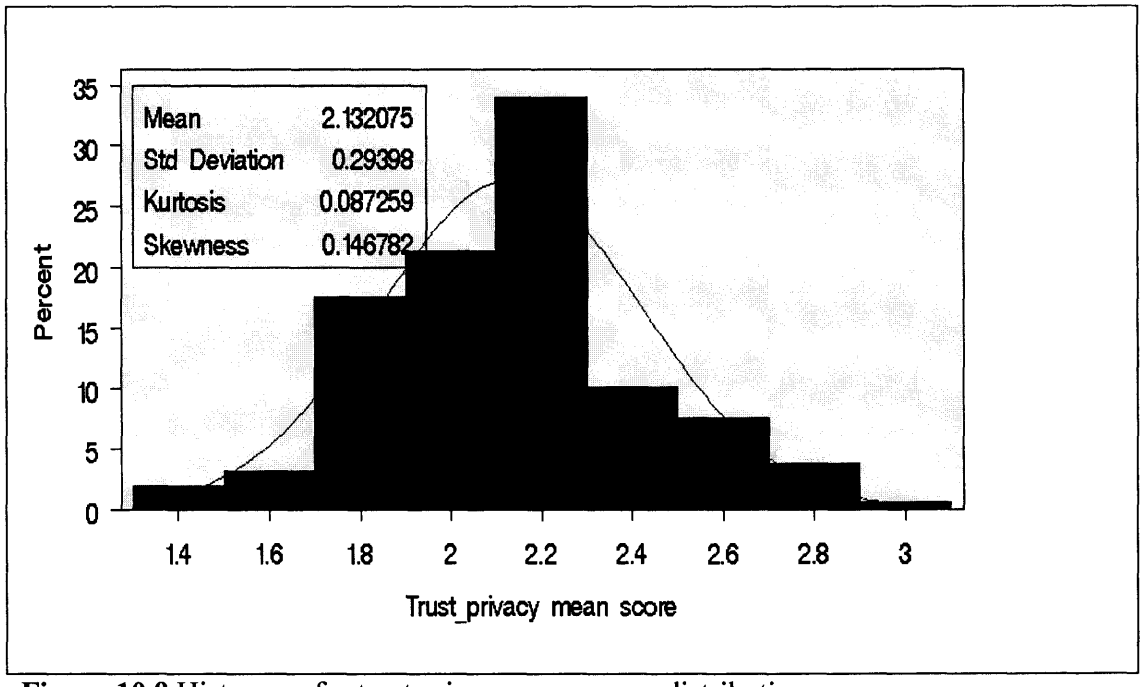

Figure 10.9 Histogram for trust privacy mean score distribution

The above is a histogram of the data distributions for the trust-privacy construct. The mean item score is 2.13 with a small standard deviation of 0.29. This shows that most of the users have concerns with trust privacy issues represented by the biometric ATM. It would seem to suggest that trust-privacy issues would need to be addressed before the introduction of the biometric ATM.

A visual observation of the histogram shows that the data is not normally distributed. The table below shows the Wilk-Shapiro test with a $p<0.0043$. This means that the null Hypothesis (H0= data normally distributed) can be rejected. The conclusion is that the data is non-normal hence non-parametric statistics will be used for this constructs.

Table **10.5** Normality Test Statistics for Trust-Privacy Construct

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.974056	Pr < W	0.0043
Kolmogorov-Smirnov	D	0.133171	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.37489	Pr > W-Sq	<0.0050
Anderson-Darling	A-Sq	1.925944	Pr > A-Sq	<0.0050

10.5.6 Descriptive Statistic and Normality Test for Social Influence Distribution

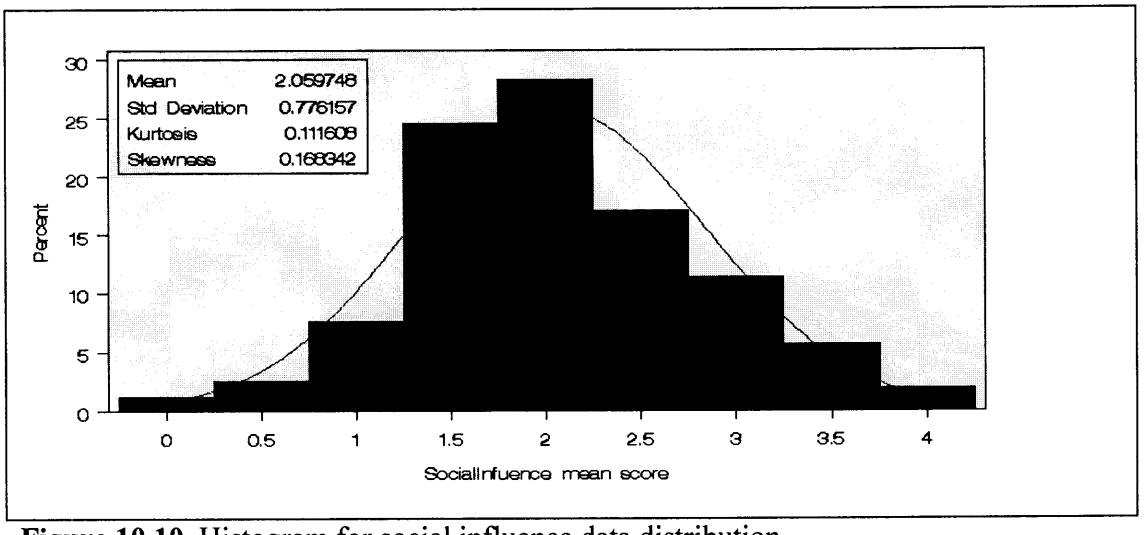

Figure 10.10 Histogram for social influence data distribution

The histogram above shows the data distribution for social influence mean item score distribution. The mean score was 2.06 while the standard deviation was 0.78. Most of the users gave low to medium scores for this construct (1.5-2.5). This would suggest that social influence did not arouse as much passion as other constructs like trust-privacy construct.

The distribution was found to be negatively skewed which was the first suggestion that the data was non-normal. This was confirmed by Wilk-Shapiro test ($p<0.0001$). Thus the null Hypothesis (H0=data is normally distributed) stood rejected. The conclusion was that the data is non-normal.

Table 10.6 Normality Test Statistics for Social Influence Construct

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.95595	Pr < W	<0.0001
Kolmogorov-Smirnov	D	0.17219	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.644699	Pr > W-Sq	<0.0050
Anderson-Darling	A-Sq	3.322779	Pr > A-Sq	<0.0050

10.5.7 Descriptive Statistics and Normality Statistics for Facilitating Conditions

The histogram below shows the data distribution for facilitating conditions construct. The mean score was 2.44 and the standard deviation was 0.67. This suggested that most of the users were neutral on facilitating conditions. A possible explanation was that on one side users have used keyboards for a long time hence are confident that they possess the necessary skill to use keyboards but on the other side they have not used the biometric keyboard hence the uncertainty.

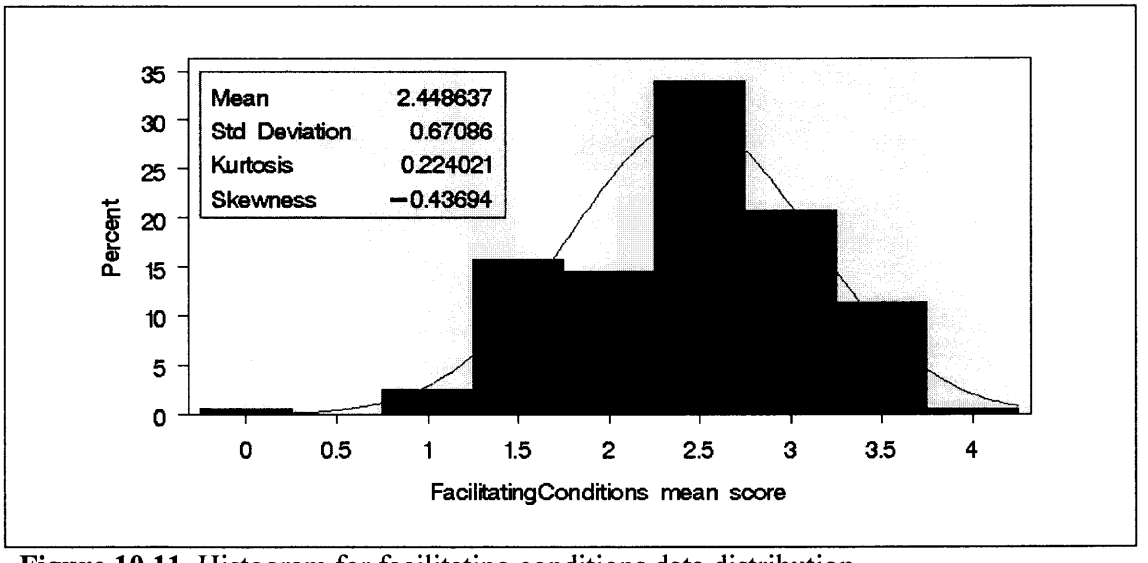

Figure 10.11 Histogram for facilitating conditions data distribution

The data distribution was negatively skewed which suggests non-normality. Wilk-Shapiro tests resulted in a $p<0.004$ hence the null Hypothesis (h0= data was normally distributed) stood rejected. The conclusion was that the data was non-normal.

Table 10.7 Normality Test Statistics for Facilitating Conditions Distribution

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.963774	Pr < W	0.0004
Kolmogorov-Smirnov	D	0.136843	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.406169	Pr > W-Sq	<0.0050
Anderson-Darling	A-Sq	2.253684	Pr > A-Sq	<0.0050

10.5.8 Descriptive Statistics and Normality Test for Behavioral Intention

The above is a histogram of the data distribution of behavioral question item mean scores. The distribution had a mean of 2.55 and a standard deviation of 0.8. There are about two peaks on the histogram. One peak is around 2.5 which represent users who were undecided in accepting and using the new biometric ATM. These users concerns would need to be addressed before introduction of the biometric ATM. The other peak was at 3.5 and represented users who were ready to accept and use the new biometric ATM. These would make the early adopters when such a product is introduced.

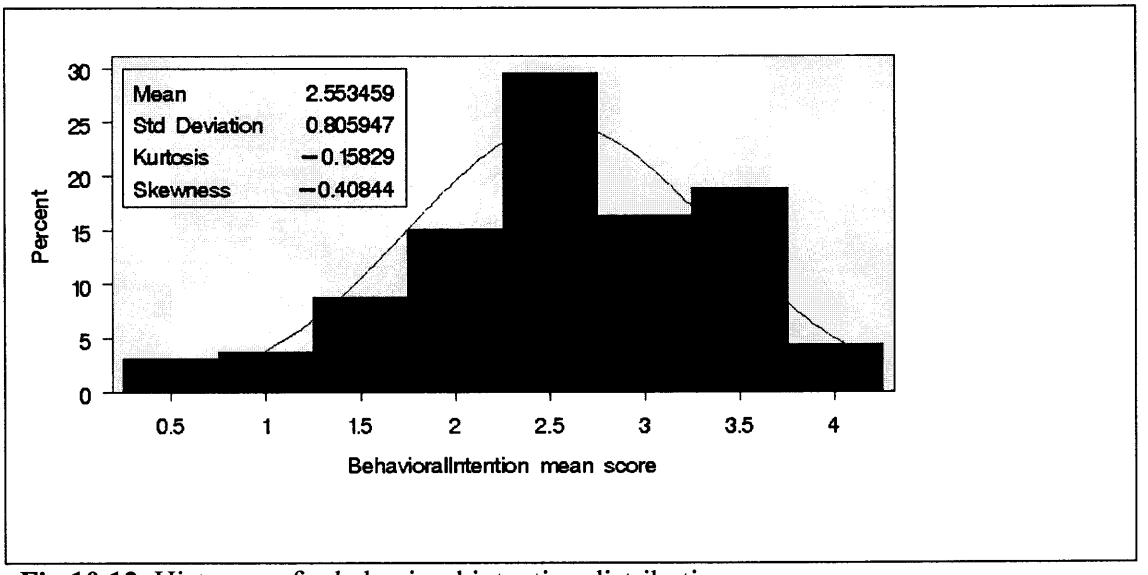

Fig 10.12 Histogram for behavioral intention distribution

The distribution was skewed to the right. The table below shows the normality test statistics. Wilk-Shapiro produces W= 0.967 and $p<0.007$. Since $p<0.05$, then the null Hypothesis that the data is normally distributed stood rejected.

Table 10.8 Normality Test for Behavioral Intention Distribution

Test	--Statistic---		-----p Value------	
Shapiro-Wilk	W	0.96685	Pr < W	0.0007
Kolmogorov-Smirnov	D	0.109313	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.279633	Pr > W-Sq	<0.0050
Anderson-Darling	A-Sq	1.666707	Pr > A-Sq	<0.0050

10.6 Background to Structural Modeling Using PLS Software

A biometric acceptance model was formulated and refined during the executive interviews as given in Chapter 9. One of the objectives of the user survey was to validate this model and this section will give the outcome of the validation.

PLS software was used for the validation of the model because the data was not Normal and the number of subjects was medium (159).

The PLS path model was implemented as recommended in (Chatelin et al. 2002). Each of the latent variables (constructs) shown in the biometric acceptance model was associated with a set of manifest variables (question items). This is the measurement model.

The structural model consisted of five latent variables (independent variables) feeding the dependent variable (behavioral intention to accept/use). This is the structural model. The biometric acceptance model is replicated here for ease of reference.

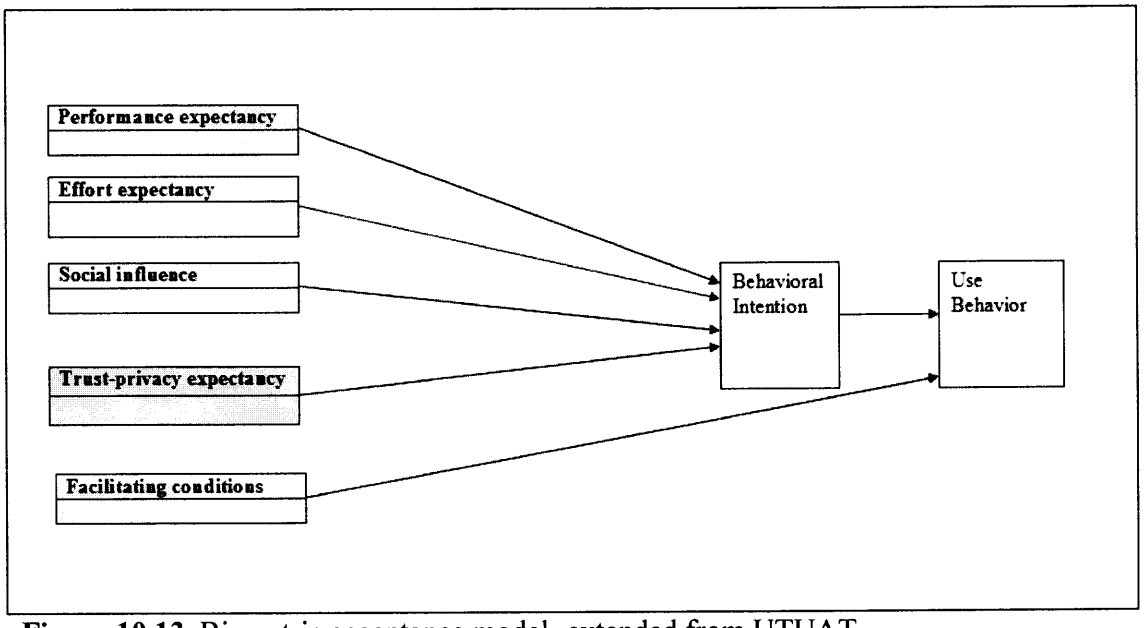

Figure 10.13 Biometric acceptance model -extended from UTUAT

The structural model equation is given as

Behavioral Intention = β_0 + β1 Performance Expectancy + β_2 Effort Expectancy +

β_3 Trust Privacy + β_4 Social Influence + β_5 Facilitating Conditions + ε

The structural equation can be written in a more compact form using the capitalized initial of the constructs as ;

$$BI = \beta_0 + \beta 1\, PE + \beta_2\, EE + \beta_3\, TP + \beta_4\, SI + \beta_5\, FC + \varepsilon \qquad \textbf{Equation 3}$$

Where β_0 = constant

β1 to β_5 = beta coefficients

ε = error term

The measurement and structural models were rigorously tested for validity and reliability as shown below.

10.7 Test of Measurement Model

The measurement model was validated by testing for; (1) Content validity, (2) Individual items reliability, (3) Construct reliability, and (4) Discriminant validity.

10.8 Content Validity

Content validity requires that the questionnaire items represent the materials (or content areas) that they are supposed to represent (Rosenthal and Rosnow 1991). This was ensured by reviewing relevant literature both from technology acceptance and biometric literature. This was followed by listing all the different concepts (represented by a sub-construct) that are used when referring to a given construct and then buildings items representing each of the sub-constructs. Thus a construct like performance expectancy was broken down to systems vulnerability, perceived security advantage and reliability.

10.9 Individual Items Reliability

Individual items reliability tests the convergence of each of the manifest question items on the latent construct that they are measuring. The manifest item should load highly on the latent construct that they are measuring but have minimal loadings on the other latent constructs that they are not measuring. Those items with less than required loadings shows that they are not good measures of the latent construct in question hence should be thrown away from the model.

Individual items reliability tests were done for all constructs using PLS. to make sure that all manifest question items converged on the latent construct that they were measuring. The usual rule is to reject item loadings less than 0.7 (Carmines and Zeller 1979) but this rule was slightly relaxed so that only items with loadings less than 0.5 were rejected due to the small sample size. Thus all manifest items with loadings less than 0.5 were thrown away of the model. The details for each construct are given below.

10.9.1 Performance Expectancy Individual Items Reliability

There were eight original question items on this latent construct with loadings as shown below

Table 10.9 Performance Expectancy Item Loadings

	SV2n	SV3n	PSA1	SV1n	PSA2	RL2n	PSA3n	RL1n
Performance expectancy	0.68	0.77	0.72	0.71	0.66	0.42	0.34	0.26
Behavior intention	0.37	0.37	0.56	0.35	0.37	0.22	0.28	0.15
Effort expectancy	-0.28	-0.33	-0.45	-0.19	-0.29	-0.42	-0.32	-0.34
Trust Privacy	0.46	0.51	0.49	0.59	0.42	0.21	0.18	0.12
Social influence	0.11	0.14	0.29	0.04	0.28	0.07	0.18	0.13
Facilitating condition	0.20	0.23	0.56	0.17	0.39	0.17	0.28	0.13

It is observed that the last three items (RL2, PSA3n and RL1n) have loadings less than 0.5 hence they were thrown out of the model. The remaining items have loading greater than 0.5 and loads highest on the performance construct while loading minimally on the other construct items. Thus they seem to be good measures of the performance expectancy construct.

10.9.2 Behavioral Intention Individual Items Reliability

There were three manifest question items on the scale with loadings as shown below. All the items in the model have factor loadings greater than 0.5 hence they were all retained in the model. They load highest on the behavioral intention construct while loading minimally on other constructs. Thus they seem to be good measures of the behavioral intention to accept and use new biometrics.

Table 10.10 Behavioral Intention Item Loadings

	BIU3	BIU2n	BIU1
Performance expectancy	0.55	0.52	0.46
Behavior intention	0.88	0.85	0.80
Effort expectancy	-0.48	-0.52	-0.39
Trust Privacy	0.58	0.56	0.51
Social influence	0.42	0.34	0.37
Facilitating condition	0.54	0.46	0.52

10.9.3 Effort Expectancy Individual Items Reliability

There were nine original manifest question items on this latent construct as shown below.

Table 10.12 Effort Expectancy Item Loadings

	TRN1	FRR1	PEE1n	FRR2n	PEE2n	RT1	RT2	TRN2	PEE3
Performance expectancy	-0.11	-0.26	-0.29	-0.24	-0.34	-0.42	-0.45	-0.37	-0.36
Behavior intention	-0.20	-0.21	-0.38	-0.27	-0.51	-0.30	-0.34	-0.31	-0.33
Effort expectancy	0.47	0.54	0.55	0.53	0.75	0.59	0.70	0.60	0.67
Trust Privacy	-0.01	-0.14	-0.34	-0.19	-0.37	-0.37	-0.36	-0.35	-0.29
Social influence	-0.24	-0.29	-0.14	-0.37	-0.38	-0.10	-0.23	-0.26	-0.07
Facilitating condition	-0.28	-0.20	-0.47	-0.37	-0.57	-0.33	-0.34	-0.34	-0.40

The first item (TRN1) has a factor loading less than 0.5 hence was thrown out of the model. All the rest were have loading greater than 0.5 and loads most on the effort expectancy construct while loading minimally on the other construct. They were thus retained.

10.9.4 Trust Expectancy Item Loadings

There were seven manifest items on this scale

All the items have loadings greater than 0.5. They loaded mostly on trust privacy construct and loaded minimally on the other constructs hence they were all retained in the model.

Table **10.13** Trust Expectancy Item Loadings

	PUD1n	TST1n	SI3n	PUD2n	TST2	SI2	SI1n
Performance expectancy	0.50	0.56	0.30	0.35	0.46	0.35	0.37
Behavior intention	0.27	0.53	0.33	0.20	0.54	0.41	0.37
Effort expectancy	-0.34	-0.37	-0.19	-0.24	-0.45	-0.19	-0.23
Trust Privacy	0.54	0.73	0.57	0.50	0.64	0.69	0.64
Social influence	0.22	0.31	-0.01	-0.07	0.28	0.05	0.05
Facilitating condition	0.21	0.33	0.12	0.15	0.52	0.28	0.25

10.9.5 Social Influence Individual Item Loadings

There were two original manifest question items on this scale.

Table 10.14 Social Influence Items Loadings

	SINF2	SINF1
Performance expectancy	0.24	0.22
Behavior intention	0.46	0.16
Effort expectancy	-0.39	-0.13
Trust Privacy	0.24	0.08
Social influence	0.96	0.55
Facilitating condition	0.49	0.18

All the social influence manifest items have loadings greater than 0.5. Each loaded highly on the social influence constructs and loaded lowly on the other constructs. Thus they seem to be good measures and were thus retained in the model.

10.9.6 Facilitating Conditions Individual Item Loadings

There were four original manifest question items on the scale.

Table 10.15 Facilitating Conditions Items Loadings

	TM1	FC3	FC1	FC2
Performance expectancy	0.52	0.09	0.33	0.19
Behavior intention	0.54	0.25	0.43	0.20
Effort expectancy	-0.54	-0.42	-0.40	-0.25
Trust Privacy	0.44	0.09	0.33	0.27
Social influence	0.46	0.31	0.30	0.05
Facilitating condition	0.82	0.53	0.74	0.39

One item (FC2) has a factor loading less than 0.5 hence was thrown out of the model. All the other manifest items had loading greater than 0.5. They loaded highly on facilitating condition construct while loading lowly on the other constructs hence were retained.

10.10 Construct Validity

Construct validity refer to the degree to which the questionnaire scale is a measure of the psychological characteristics of interest (Cronbach and Meehl 1955). The goal of construct validity or internal consistency is to confirm that the scale is really measuring the concept/ construct that it is claiming to measure. This is attained by investigating the agreement between the measurement items in the scale and the theoretical construct. To what extent do the items in the scale focus on the notion of the construct?

One way of proving that measures have construct validity is to prove that they have both convergent and discriminant validity. Convergent validity shows that measures that are supposed to be related are practically related while discriminant validity shows that measures that are not supposed to be related are indeed practically not related (Cronbach and Meehl 1955; Rosenthal and Rosnow 1991).

The most common measure is Chronbach alpha. However Fornell and Lacker measure was used in this study as it is preferred compared to Chronbach alpha when doing structural modeling since it computes the items loadings from the causal model (Fornell and Larcker 1981). Construct reliability should be at least 0.7 (Nunnally 1978)

The formulae for computing construct reliability for the PLS model is (Chatelin et al. 2002) .

Construct reliability = $[(\text{SUM}\ (sl_i))^2]/[(\text{SUM}(sl_i))^2 + \text{SUM}(e_i))]$ **Equation 4**

Where sl_i = standardized loadings for the indicators for a particular latent variable

e_i = corresponding error terms, where error is 1 minus the reliability of the indicator, which is the square of the indicator's standardized loading. This formula was applied to all the constructs and the following were the construct reliability values.

10.10.1 Construct Reliability for Behavioral Intention

Table 10.16 Construct Reliability for Behavioral Intention

Items	Original loading	Bootstrap loading	Standard error	T	P-value	Construct reliability
BIU3	0.42	0.42	0.02	18.38	0.000	
BIU2n	0.39	0.39	0.02	19.60	0.000	
BIU1	0.37	0.37	0.02	17.07	0.000	
Sum	1.18		0.06			**0.96**

The tables above shows that there is a high agreement between the measurements manifest variables and the theoretical behavioral intention to accept a new biometric construct. This validates that the manifest variable are good measure of the construct.

10.10.2 Construct Reliability for Performance Expectancy

Table 10.17 Construct Reliability for Performance Expectancy

Items	Original loading	Bootstrap loading	Std. Error	T	p-value	Construct reliability
SV2n	0.25	0.26	0.03	7.17	0.000	
SV3n	0.25	0.24	0.03	7.83	0.000	
PSA1	0.38	0.38	0.04	8.71	0.000	
SV1n	0.24	0.23	0.04	6.59	0.000	
PSA2	0.25	0.25	0.05	5.52	0.000	
Sum	1.37		0.13			**0.94**

There is a high agreement between the manifest variables and the theoretical performance expectancy construct. The construct reliability for performance expectancy is higher than the recommended minimum (0.7) which shows that the construct is convergent.

10.10.3 Construct Reliability for the Effort Expectancy Construct

Table 10.18 Construct Reliability for Effort Expectancy

Items	Original loading	Bootstrap loading	Standard error	T	P-value	Construct reliability
FRR1	0.12	0.11	0.04	2.92	0.002	
PEE1n	0.23	0.22	0.04	5.08	0.000	
FRR2n	0.16	0.16	0.04	3.66	0.000	
PEE2n	0.31	0.30	0.04	7.94	0.000	
RT1	0.18	0.19	0.04	4.57	0.000	
TRN2	0.18	0.19	0.04	5.18	0.000	
PEE3	0.20	0.19	0.04	5.66	0.000	
RT2	0.20	0.20	0.03	6.08	0.000	
Sum	1.58		0.31			**0.89**

The tables above shows the construct reliability values for effort expectancy construct. There seems to be a high agreement between the manifest variables and the theoretical construct that they are supposed to measure. The reliability value is much higher than the required minimum of 0.7.

10.10.4 Construct Reliability for Trust Privacy Construct

Below are the construct reliability values for Trust privacy construct.

Table 2.19 Construct Reliability for Trust Items

Items	Original loading	Bootstrap loading	Standard error	T	P-value	Construct reliability
PUD1n	0.16	0.16	0.04	3.84	0.000	
TST1n	0.32	0.33	0.04	8.43	0.000	
SI3n	0.20	0.19	0.04	5.20	0.000	
PUD2n	0.12	0.11	0.04	2.68	0.004	
TST2	0.32	0.33	0.04	7.35	0.000	
SI2n	0.24	0.23	0.04	6.82	0.000	
SI1n	0.22	0.22	0.03	6.97	0.000	
Sum	1.57		0.27			**0.90**

The construct reliability value is 0.9 which is far above the required minimum of 0.7. Thus there is a high agreement between the manifest variables and the trust privacy construct that they are supposed to measure

10.10.5 Construct Reliability for Social Influence Construct

Table 3 Construct Reliability for Social Influence Items

Items	Original loading	Bootstrap loading	Standard error	Original loading	P-value	Construct reliability
SINF2	0.87	0.88	0.08	0.87	0.000	
SINF1	0.30	0.25	0.14	0.30	0.015	
Sum	1.17		0.22	1.17		0.86

The table below shows that the construct reliability coefficient for social influence construct is 0.86 which is above the minimum 0.7.

Thus there is a high agreement between the manifest variables and the theoretical construct.

10.10.6 Construct Reliability for Facilitating Conditions Construct

The construct reliability value is 0.9 which is far above the required minimum of 0.7.

Table 10.21 Construct Reliability for Facilitating Condition Items

Items	Original loading	Bootstrap loading	Standard error	T	P-value	Construct reliability
TM1	0.59	0.59	0.06	9.61	0.000	
FC3	0.28	0.29	0.08	3.67	0.000	
FC1	0.47	0.45	0.06	7.36	0.000	
	1.34		0.20			0.90

There is a high agreement between the manifest variables and the theoretical construct.

10.10.7 Conclusion

All the given manifest variables had a high agreement (<0.85) with the theoretical constructs that they were supposed to measure. This shows that they are good measures of the constructs that they were supposed to measure.

10.11 Discriminant Validity

Discriminant validity checks whether the construct is different from the other constructs. Measures that are supposed to be related should in practice correlate well together and not correlate to dissimilar measures.

The table below shows the correlation values for manifest variables measuring their constructs as well as the correlation with other constructs

Table 10.22 Discriminant Validity

	Performance expectancy	Behavior intention	Effort expectancy	Trust privacy	Social influence	Facilitating conditions
Performance expectancy	0.73					
Behavior intention	0.33	0.85				
Effort expectancy	0.21	0.31	0.62			
Trust Privacy	0.45	0.42	0.25	0.62		
Social influence	0.06	0.20	0.14	0.05	0.78	
Facilitating condition	0.19	0.35	0.38	0.19	0.25	0.73

It is observed that measures of each of the constructs relate well with that theoretical construct through high correlations and do not relate much to the other constructs. Thus it would seem like the measures for this study have high discriminant validity.

Since the measures have been shown to have both a high convergent validity and a high discriminant validity then it can be deduced that they have high construct validity.

10.12 Test of Structural Model

The following Hypothesis were proposed as corollary to research question two as given in Chapter 3

There will be a positive correlation between behavioral intention to use

and

H2a: Performance expectancy

H2b: Social influence

H2c: Facilitating conditions

H2d: Trust privacy expectancy

There will be a negative correlation between behavioral intention to use and H2e: Effort expectancy

These hypotheses are mathematically represented by the structural equation model given earlier and duplicated below for ease of reference.

Behavioral Intention = β_0 + β1 Performance expectancy + β_2 Effort expectancy + β_3 Trust Privacy + β_4 Social Influence + β_5 Facilitating conditions + ε

Where β_0 = constant

β1 to β_5 = beta coefficients

ε = error term

The data was processed using PLS and resulted in the following model with beta coefficients as shown.

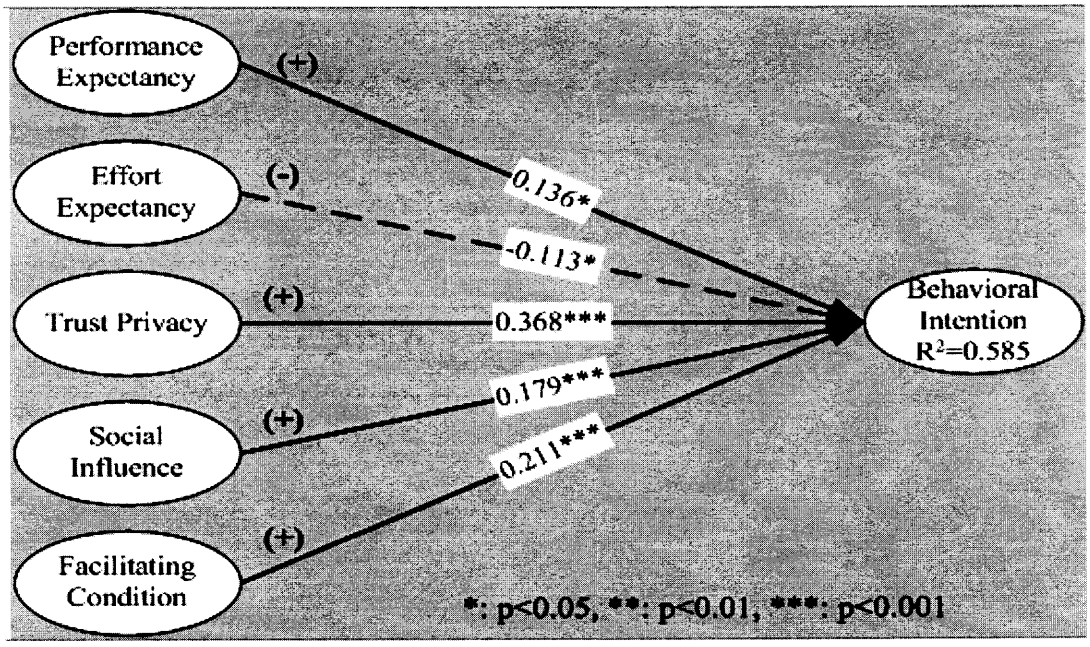

Figure 10.14 Biometric acceptance model

A summary of the beta coefficient and associated statistics is given below

Table 10.23 Structural Equation Model Coefficients

	Performance expectancy	Effort expectancy	Trust Privacy	Social influence	Facilitating conditions
Beta coefficients	0.14	-0.11	0.37	0.18	0.21
t	1.78	1.65	4.90	2.77	2.81
p-value	0.04	0.05	0.00	0.00	0.00

10.12.1 Implication of Results on Proposed Hypothesis

The following inference can be made from above results:

H2a: There will be a positive correlation between behavioral intention to use and performance expectancy.

The beta coefficient for this Hypothesis = $\beta 1 = 0.14$ from the model. The beta was statistically significant (t=1.78, p=0.04, n =499 bootstraps)

The inference is that the results of the user survey support this Hypothesis as proposed.

H2b: There will be a positive correlation between behavioral intention to use and social influence.

The beta coefficient for this Hypothesis = $\beta 4 = 0.18$ from the model. The beta was statistically significant ($t=2.77$, $p<0.001$, n =499 bootstraps)

The inference is that the results of the user survey support this Hypothesis as proposed.

H2c: There will be a positive correlation between behavioral intention to use and facilitating conditions.

The beta coefficient for this Hypothesis = $\beta 5 = 0.21$ from the model. The beta was statistically significant ($t=2.81$, $p<0.001$, n =499 bootstraps)

The inference is that the results of the user survey support this Hypothesis as proposed.

H2d: There will be a positive correlation between behavioral intention to use and trust privacy expectancy.

The beta coefficient for this Hypothesis = $\beta 3 = 0.37$ from the model. The beta was statistically significant ($t=4.9$, $p<0.001$, n =499 bootstraps)

The inference is that the results of the user survey support this Hypothesis as proposed.

H2e: There will be a negative correlation between behavioral intention to use and effort expectancy.

The beta coefficient for this Hypothesis = $\beta 2 = -0.11$ from the model. The beta was statistically significant ($t=1.65$, $p=0.05$, n =499 bootstraps)

The inference is that the results of the user survey support this Hypothesis as proposed.

10.12.2 Conclusion

The conclusion is that the proposed hypothesis were validated .

10.13 Test of Mediating Variables on The Biometric Model

The histograms showing data distribution for the model constructs demonstrated that some of the data distribution had more than one main peak. This suggested some heterogeneity in the user population. Further investigation was conducted to see what could be causing such distributions.

The study investigated the mediating effects of several variables both from the original UTAUT model as well as from the demographics.

10.13.1 Experience as a Mediating Variable

Experience was operationalized as computer usage. Subjects were asked to indicate how often they used computers per week. They were required to give a breakdown of hours used to email, program, browse and type per week. The total number of hours of computer usage per week was computed and a histogram of the usage made as shown below.

It was observed that there were two main peaks one at 40 hours/week usage and another at 100 hours/week usage. It appeared like the population was made up of to two distinct sets of groups. The mid-point of 80 hours per week was taken as the dividing point hence all the subjects were dived into two group one with computer usage>80 hours per week called experts and the other with less than 80 hours per week labeled as novices.

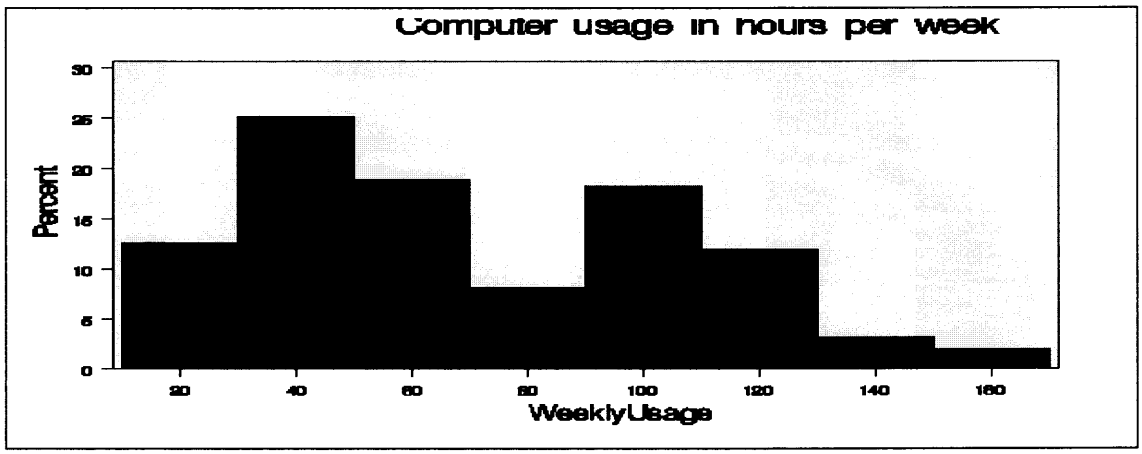

Figure 10.15 Computer usage in hours per week for all subjects

The next stage of the investigation was to investigate the variations in user perception on all the constructs in the biometric acceptance model between the two distinct experience groups.

The constructs data distributions were all non-normal (refer to check for normality section above) hence the parametric t-test could not be used to compare the means of the experts and novices.

Rather, the equivalent non-parametric Wilcoxon-Mann-Whitney test was used. The test does not require interval data or normal distribution. The test only assume that data is ordinal which was met in this study from use of likert scale ranked data (Conover 1999).

Table 10.24 Effect of Experience on Model

Construct	Skill level	No. of subjects	Mean rank score	Z-score	p-value
Performance expectancy	Experts	63	88.5	1.9	0.057
	Novices	96	74.4		
Trust Privacy	Experts	63	82.5	0.55	0.58
	Novices	96	78.4		
Effort expectancy	Experts	63	79.7	-0.067	0.95
	Novices	96	80.2		
Behavioral intention	Experts	63	92	2.8	0.005
	Novices	96	71		
Social influence	Experts	63	79	0.12	0.9
	Novices	96	80		
Facilitating conditions	Experts	63	82	0.59	0.56
	Novices	96	78		

It was observed that computer experts (those who use computers more than eighty hours per week) had a higher score on their behavioral intention to accept the biometric keyboard. This difference was statistically significant (Z= 2.8, p=0.0047, n=159).

There was also an almost significant difference between the experts and novices on the performance perceptions (z= 1.9, p=0.057, n=159) where the experts perceived the performance of the biometric ATM to be higher (mean =88.5) while the novices perceives the perception of the biometric to be lower (mean score = 74.4)

The combined effect was that experts perceived a higher performance from the biometric ATM hence are more likely to adopt while novices perceives a lower performance hence are less likely to accept the biometric.

The implication for the above is that organizations introducing biometric keyboards should give more attention to irregular computer users as the later have more issues with new technology. Possible explanations would be a higher level of anxiety on the novices.

The experts are comfortable with computers hence feel more confident with new technologies.

10.13.2 Effect of Gender as a Mediating Variable

Subjects had been asked to state their gender in the demographic section. An investigation was carried out to find the effect of gender on the constructs in the biometric model as shown below.

It was observed that males' performance expectancy on the biometric keyboard was higher than that of the females with mean rank scores of 84.6 and 70 respectively. This difference is statistically significant (z=1.962, 0.05, n=159)

Females had issues with the performance expectancy of the biometric keyboard which would need to be addressed before such a technology is introduced.

Table 10.25 Effect of Gender on Models Constructs

Construct	Gender	Subjects	Mean rank score	Z-score	p-value
Performance expectancy	Male	112	84.6	1.962	0.0514
	Female	47	70		
Effort expectancy	Male	112	86.5	0.200	0.84
	Female	47	78.9		
Trust privacy	Male	112	82.6	-1.12	0.26
	Female	47	73.7		
Behavioral intention	Male	112	82.8	-0.1.21	0.228
	Female	47	73.2		
Social influence	Male	112	76.9	1.32	0.184
	Female	47	87.3		
Facilitating conditions	Male	112	78.2	0.731	0.46
	Female	47	84		

10.13.3 Effect of Major as a Mediating Variable

Table 10.26 Effect of Major as a Mediating Variable

Construct	Major	Subjects	Mean rank score	Z-score	p-value
Performance expectancy	Computing	132	79.5	0.32	0.74
	Nursing	27	82.6		
Effort expectancy	Computing	132	79.3	0.38	0.70
	Nursing	27	83.1		
Trust privacy	Computing	132	82.98	-1.83	0.07
	Nursing	27	65.43		
Behavioral intention	Computing	132	81.3	-0.82	0.41
	Nursing	27	73.42		
Social influence	Computing	132	79.9	0.04	0.96
	Nursing	27	80.33		
Facilitating conditions	Computing	132	81.02	-0.62	0.53
	Nursing	27	74.98		

The table above shows statistics for the mediating effect of major on the entire model constructs. The effect of major (nursing students/ computing major) does not seem to have any significant mediating effects on any of the given constructs.

However the mediating effect on the trust-privacy construct are almost significant ($p=0.07$). The dissertation speculates that it is only because there were not enough nurses otherwise it would seem that nurses have less trust (mean score =65) on the biometric ATM than those of computing majors with mean score = 82.98.

10.13.4 Search for other Mediators

Several other mediators were tested. The effect of Age of subject, frequency of ATM usage per week and the total period that users have had an ATM were all tested for mediating effects. There were no significant mediating effects on any of the model's constructs.

10.14 Summary

The chapter set out to validate the biometric acceptance model formulated during the executive interviews study. The measurement and structural models were both validated. The entire five proposed hypothesis were supported by the results.

The second objective for the study was to find acceptable parameter to users of biometric keypad as per the research sub-questions given in the research questions Chapter 3. Research sub-question 10 sought to investigate the number of training iterations that users were willing to engage in to generate data to develop the keypad. The results indicated that this will at most be ten iterations. Researches sub-question 11 sough to investigate the acceptable false rejection rates under various circumstances. The results indicated that will not go beyond two. The table below is a summary of the above.

Table 10.27 Answers to research-sub-question 10-11

10	How many training iterations is a typical user willing to engage in to generate data to develop their personal biometric keypad classifier?	Users are unlikely to want to train more than once and only for a maximum of ten iterations		Chapter 10 – user survey results
11	What is an acceptable false rejection rate under various user circumstances?	Users are unlikely to accept more than 2 false rejection rates		Chapter 10 – user survey results

The chapter gave results for the user attitude survey starting from the descriptive statistics, the validation of the model and the mediating effects of several variables.

Most of the users surveyed indicated that they would not be willing to pay extra fee for a working biometric even if it helped reduce fraud.

CHAPTER 11

DISCUSSIONS AND CONCLUSIONS

11.1 Introduction

This chapter presents the series of results that were obtained through the research presented in this dissertation. The results are discussed in relationship to the research questions posed in Chapter 3. In effect, this chapter does not discuss the individual hypotheses that were tested in the various experiments conducted, but rather covers the larger issue of how much do we now know about the research area and the research questions we tried to answer. Both the conclusion of the results presentation and the suggestions for future work address the over riding question which is, "Is it viable to develop and introduce a keypad biometric?" In particular, what do we know now about this viability and what do we need to find out to further answer this question? This is followed by a summary of the key contributions of the research and a discussion of the research limitations. Finally suggestions are given for future research with the goal of extending several findings from this dissertation.

11.2 Overall Synthesis and Conclusions

This dissertation addresses two major research questions which were broken into fifteen sub-questions. Table 11.1 summarizes the results from investigating these sub-questions. The source of the results is summarized in the two right most columns in this table, that is, either from research conducted in the dissertation, from prior literature or a combination of both of these methods. Of the research sub-questions posed, sufficient

information was obtained to give a viable answer to all but sub-questions 7 and 9. In sub-question 7, the subjects in the experiment all had low typing speeds so that the range of typing speeds was not sufficiently sampled to determine how it impacted classification rates. In sub-question 7, there was a suggestion that PIN configuration affected classification accuracy but that the effect was small for a keypad. This result, too, will need further investigation.

The two major questions addressed were:

RQ1: What is the technical feasibility of performing authentication at the keyboard gateway?

and

RQ2: What are the critical factors that would determine the acceptance of a new biometric technology similar to the biometric keypad?

Sub-questions 1-11 address the first research question. Although it has been shown that a keypad biometric can be built and perform relatively accurate classification, there are some issues that need to be addressed in its development. First, because typing skill does affect classification accuracy (sub-question 7), there is a suggestion that the keypad biometric might not work for all people. This has to be further investigated since it is not known if continued use of a keying pattern, even by poor typists, will eventually stabilize enough to improve classification accuracy for this class of users. Second, user responses to the number of training trials they are willing to accept (sub-question 10) and the number of false rejection rates they are willing to accept (sub-question 11) set some severe restrictions on the system. For training, it may be that biometric classification can only begin to occur after a user has done some given number of entry trials with the

system, that is, while they are using the actual system in the real world.. It may also be that the system will never work for some users and that after some number of classification trials, a system will mark a user as "unable to classify" and therefore use traditional authentication means only.

Third, because elapsed time has been shown to affect classification accuracy (sub-question 8), some form of continuous capture and retraining needs to be built into the biometric keypad if it is to not have significant false rejection rates. This is one of the most serious problems uncovered in the technical feasibility investigation and has to be studied further. It may be that long term usage of a PIN removes this issue.

Research Question 2 is addressed by sub-questions 12-15. The key factor found in acceptance of the technology was addressed in sub-questions 12 and 15. This was trust and privacy. The results suggest that end users have key concerns about these issues which might affect the deployment of this technology to the general public. It may be that keypad biometrics are not likely to work for ATM machines but may work for authenticating users working in critical industries where access to financial data or personal data needs to be controlled.

Table 11.1 Summary of Research Results from Dissertation

No.	Research sub-questions to be investigated	Answer to research sub-question	Source	
			Lit Review	Dissertation Research
1	Are individual typing patterns unique for a numeric keypad using a small (4-6 digit) number for authentication?	Yes they are unique. Attained 90% classification from 4 subjects		Chapter 4 – classifier development
2	What are the optimal characteristics of the input signals that should be used for classification of different users?	Inter-key time, key-down time and pressure matched using wavelet coefficients	Lit Review	Chapter 4 – classifier development
3	What method is best for characterizing the pattern differences produced by individual typists?	Support Vector Machine	Lit Review	Chapter 4 – classifier development
4	Which are the most appropriate classifiers for biometric keypads?	Combined pressure, inter-key time and key down time	Lit Review	Chapter 6 – post hoc analysis
5	How should a pressure keypad be built and sampled to provide pressure data to the classifier engine?	Pressure causes a voltage change which is sampled and used for classification		Chapter 4 – keypad development
6	Would the addition of pressure pattern features to the time pattern features improve discrimination accuracy?	Yes, adding pressure improves discrimination accuracy		Chapter 6 – post hoc analysis
7	How much will variations in typing speed impact classification performance?	Typing speeds below 30 words per minute reduce classification accuracy		Chapter 6 - post hoc analysis

Table 11.1 Summary of Research Results from Dissertation (Continued)				
8	What is the effect of elapsed time on the classification performance?	Elapsed time significantly reduces classification performance		Chapter 6 - experiment
9	Are there differences in classification performance for different pin numbers?	Not found in study conducted but data suggests that differences may exist. The effect may be small		Chapter 6 - experiment
10	How many training iterations is a typical user willing to engage in to generate data to develop their personal biometric keypad classifier?	Users are unlikely to want to train more than once and only for a maximum of ten iterations		Chapter 10 – user survey results
11	What is an acceptable false rejection rate under various user circumstances?	Users are unlikely to accept more than 2 false rejection rates		Chapter 10 – user survey results
12	What critical acceptance factors do executives believe will impact end user acceptance of a keypad biometric?	Executives believe performance, ease of use and trust and privacy will be the major factors.	Lit Review	Chapter 8 – results from interview
13	To what extent will the critical adoption factors presented in the research literature impact adoption for a keypad biometric?	The key adoption factors are perceived end user acceptance of the technology, cost and performance	Lit Review	Chapter 8 – results from interview
14	What, if any, new factors will affect executive adoption of the keypad biometric?	Cost was the primary new factor that came up		Chapter 8 – results from interview
15	What factors will affect the acceptance of the biometric keypad by the end user?	The UTAUT factors adapted for biometric issues and trust / privacy	Lit Review	Chapter 10 – user survey results

Overall this dissertation has accomplished two things in addressing the research sub-questions shown in Table 11.1. First, it has brought about new knowledge about a specific innovation designed to thwart identity fraud. It has also, in its own process, outlined a business method for examining such a problem and finding out both what the solutions are to building a biometric authentication system but also what the issues are that need to be resolved.

The dissertation was designed to answer some of the product development questions that designers of information systems are forced to deal with. The product development process shown below is a long and costly process in terms of capital and manpower investment. To minimize the risk of failure, there is need to take a holistic approach in the design and introduction of new technologies. The dissertation work can be viewed as a template that can be used by later day researchers in addressing several stages of the product development cycle shown below.

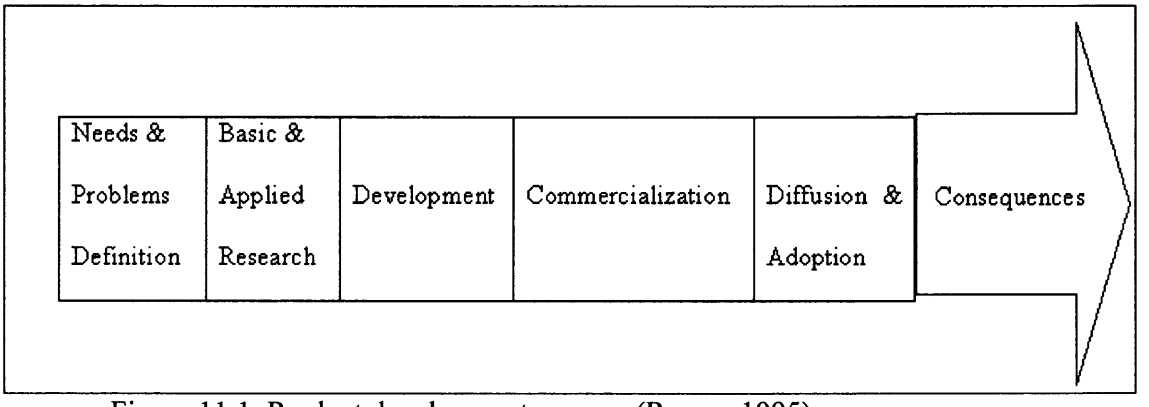

Figure 11.1 Product development process (Rogers 1995)

The first two chapters of the dissertation addressed the first stage of needs and problem definition to define the problem of identity fraud. Several outstanding issues that have made identity fraud rampant were presented. Chief among these issues was the

current inadequate authentication. The key problem was defined as the use of external identifiers which can be easily lifted or separated from the owner. A need for incorporating biometric identifiers which cannot be easily separated from the self was identified. Several biometrics were considered and the keyboard based authentication identified as a method that could potential fit the need but was still in the early stages of research.

The research questions that drove the rest of the dissertation were defined in Chapter three. The first research question was to investigate the technical feasibility of keyboard based authentication while the second research question was to identify the critical factors that would determine the success or failure of keyboard based authentication. Three studies were designed to answer these research questions.

The first study addressed the stage of basic and applied research in the product development process shown above. The study investigated the technical feasibility of keyboard based authentication. The results verified that it is technically feasible to authenticate users at the keyboard although there are some limitations.

The second and third studies involved looking ahead at the diffusion and adoption stage and investigating the critical factors necessary for the adoption of the keyboard biometric. The rationale looking ahead is the realization that there are many paths that can move the prototype from the basic/applied to the diffusion stage yet not all would be successful and the design would not know before hand the optimal path to take.

The second study identified several factors as important for successful adoption. Further the executive interviews resulted with a ranking of all the critical factors. The top three factors were performance, ease of use and trust-privacy issues. Knowing the top

three factors by itself gives the designer a head start over the competition. The executives were also asked to give their opinion on the strengths and improvement that could be made on the biometric keyboard. The greatest strength of the biometric keyboard was identified as its ease of use while the greatest concern was identified as the performance of the biometric keyboard. Several suggestions were given to make the prototype better. These suggestions can be fed back into the first study and used to make a second generation prototype that leverage the given strengths but also implements the suggested improvements. Several hypotheses were proposed to govern the relationships between the critical factors identified from the study and the behavioral intention to adopt the biometric keyboard. These hypotheses created the basis for formulating the biometric acceptance model.

The third study set out to investigate the user perceptions on the critical factors identified in study two. The aim was to confirm the Hypothesis and validate the model formulated from study two. Further the study also wanted to measure the acceptable parameters for the biometric keyboard prototype. Thus the study was partly an extension of study two and partly a feed back loop to study one.

The third study validated the suggested biometric acceptance model and confirmed the proposed Hypothesis. Thus, the study confirmed that performance expectancy, trust-privacy level, social influence and facilitating conditions were positively correlated to the behavioral intention to accept new technologies like the biometric keyboard. Like wise the study confirmed that effort expectancy has a negative correlation with the behavioral intention to accept and use a new technology.

The message to designers was simple. If you want your innovation accepted by users, then make sure that: (1) the innovation has a high performance. (2) The innovation is trustworthy and does not intrude on user privacy. (3) Make sure the facilitating conditions are in place and the timing is right. (4) The innovation is a cool technology to use. (5) Make sure the effort expectancy is low.

Thus the results from study three gives the designer in study one, a yard stick to evaluate the progress being made and to predict the expected level of acceptance that would result. The conclusion is that the whole dissertation is in reality addressing the same problem in a multi-faceted approach.

11.3 Dissertation Contributions

This dissertation reviews and synthesizes the current efforts going on in the fight against identity fraud.

Pertinent issues that need to be addressed in mitigating identity fraud were identified key among which was the problem of inadequate authentication. The shortcomings of current authentication methods were examined and a keyboard-based authentication prototype solution suggested after a consideration of several other technologies which may also be viable in other circumstances.

A biometric keypad was developed which demonstrated the feasibility of the solution and also provided a template to future designers of biometric systems. The biometric keypad was then evaluated under different field conditions that the user population of such keypad are bound to face.

The keying patterns were shown to vary with elapsed time which had major design implication for all biometrics. The choice of the personal identification number was also found to have some effect although this was not statistically significant probably due to the small effect size and subjects. The classification rates from the biometric keypad were found to depend on the experience of the user which implies that users should be trained as much as possible.

The critical important factors in the acceptance of biometrics were shown to be performance, ease of use and trust- privacy issues. Ease of use and cost were shown to be the most desired attributes of the keypad and suggestions made on improving the performance of the biometric.

A biometric acceptance model was formulated and validated which can henceforth be used as a yardstick in evaluating other biometrics and security products. The critical factors determined and validated can also be used to create a basis for interventions in the marketing strategy if any of the important factors is not doing well. They can also be used to design interventions to increase adoption and redesign new technologies to fit user expectations.

New measurement scales applicable to biometrics developed for performance expectancy, effort expectancy and trust-privacy construct by redefining the constructs to apply to biometrics.

11.4 Limitations

11.4.1 Limitations to Research Question 1: Technical Feasibility

A single keyboard was used for all the testing in research question one. While the methods used are generalizable, the data obtained may have some variations since each keyboard characteristic may be unique. A second limitation is the small population used and also the use of student population.

11.4.2 Limitations to Research Question 2: Executive Interview

This was an exploratory study and the four executives studied were too few to be representative of the general population. Further theoretical saturation point was not reached hence there is still a possibility that the number of factors suggested were not exhaustive.

11.4.3 Limitations to Research Question 2: User Survey

There was an overemphasis in items used to test performance expectancy, effort expectancy and trust-privacy expectancy at the expense of social influence and facilitating conditions.

11.5 Future Work

The results obtained from dissertation research addressed the questions designed in the research design chapter. However these results and finding can be extended and improved. A possible improvement would be the detection and removal of outliers to see if classification will improve. An analysis of the confusion matrixes to identify subjects that were continuously confused would also lead to improved classification. A possible solution to the changing patterns with elapsed time can be the incorporation of a learning mechanism to see if the classifier can learn with changing behavioral patterns. This will be addressed in a future research.

The fusing of pressure and time classifiers inputs was done by combining the two sets of features. An improved method would be the investigation of a linear combination of parameters to the classification parameter to fuse the output of the pressure and time input features classifiers via a voting mechanism in a future study.

The biometric user acceptance model validated using a keypad. A future study will cross-validate the model with another biometric product or with population to examine the generalizability of the model.

11.6 Summary

This chapter synthesized the results of the three studies. A thread was established that connects all the different sections of the dissertation to show that the whole dissertation is coherent and parsimonious. The chapter then gives the contributions and limitations of the dissertation research. Finally, suggestions are given for future research with the goal of extending several finding from this dissertation.

APPENDIX A RQ1- SUBJECTS INSTRUCTIONS SHEET

Thank you for agreeing to participate in the experiment.

The aim of the experiment is to study the behavioral patterns of test takers.

The experiment follows a four-step process and will approximately take 30 minute

The five steps are:

Fill in the consent form.

Fill in the pretest questionnaire.

Under go a typing speed test conducted by the researcher

Undergo training on answering the Quiz.

APPENDIX B RQ1-PRETEST BACKGROUND QUESTIONNAIRE

1. Your Pseudonym: _____

2. Pseudo Id_____

3. Your gender: ___ Male ___ Female

4. Your Age Group: _____18-25 _____26-33 _____34-41 _____42 and above

5. Computer usage

Table B.1 Computer Usage				
Computer Activity per week	Less than 10Hrs	10-20 Hrs	>20 and <= 40 Hrs	>40 Hrs
Email				
Programming				
Web Browsing				
Typing				
Total				

6. Your keyboard typing speed from the conducted typing test is _____

7. How many fingers do you use to type.

☐ Two-finger ☐ 4 finger ☐ Touch typist(10 fingers)

8. Do you look at the keyboard when typing?

☐ Always ☐ Often ☐ Sometimes ☐ Rarely ☐ Never

9. How often do you use an ATM machine in a week?

☐ Never ☐ Rarely(<1 time) ☐ 1-2 times ☐ 3-4 times

☐ **> 4 times**

10. For how long have you used an ATM machine?

☐ **< 3 Months** ☐ 3-12 Months ☐ **>12 months**

APPENDIX C RQ1-CONSENT FORM

NEW JERSEY INSTITUTE OF TECHNOLOGY

323 MARTIN LUTHER KING BLVD.

NEWARK, NJ 07102

CONSENT TO PARTICIPATE IN A RESEARCH STUDY

TITLE OF STUDY: Electronic capture and analysis of fraudulent behavioral patterns: An application to identity fraud

RESEARCH STUDY:

I,_____, have been asked to participate in a research study under the direction of ___Benjamin Ngugi ___

Other professional persons who work with them as study staff may assist to act for them.

PURPOSE: The purpose of the experiment is to better understand human behavioral patterns when typing

DURATION:

My participation in this study will last for thirty minutes

PROCEDURES:

I have been told that, during the course of this study, the following will occur:

A background questionnaire will be presented for me to answer

A typing speed test will be administered.

Training will be provided to make me conversant with the world trivia self test program.

I will then answer twenty world trivia quiz questions

PARTICIPANTS:

I will be one of about _____50_____participants to participate in this trial.

EXCLUSIONS:

I will inform the researcher if any of the following apply to me:

- I do not wish to participate in the experiment and no questions will be asked

RISK/DISCOMFORTS:

I have been told that the study described above may involve the following risks and/or discomforts:

There are no known risks or any anticipated risks

There also may be risks and discomforts that are not yet known.

I fully recognize that there are risks that I may be exposed to by volunteering in this study which are inherent in participating in any study; I understand that I am not covered by NJIT's insurance policy for any injury or loss I might sustain in the course of participating in the study.

CONFIDENTIALITY:

Every effort will be made to maintain the confidentiality of my study records. Officials of NJIT will be allowed to inspect sections of my research records related to this study. If the findings from the study are published, I will not be identified by name. My identity will remain confidential unless law requires disclosure.

PAYMENT FOR PARTICIPATION:

I have been told that there will be NO monetary compensation for my participation in this study.

RIGHT TO REFUSE OR WITHDRAW:

I understand that my participation is voluntary and I may refuse to participate, or may discontinue my participation at any time with no adverse consequence. I also understand that the investigator has the right to withdraw me from the study at any time.

INDIVIDUAL TO CONTACT:

If I have any questions about my treatment or research procedures that I discuss them with the principal investigator. If I have any addition questions about my rights as a research subject, I may contact:

Dawn Hall Apgar, PhD Chair, IRB (973) 642-7616

SIGNATURE OF PARTICIPANT

I have read this entire form, or it has been read to me, and I understand it completely. All of my questions regarding this form or this study have been answered to my complete satisfaction. I agree to participate in this research study.

Subject Name:_____ Signature:_____

Date:_____

SIGNATURE OF READER/TRANSLATOR IF THE PARTICIPANT DOES NOT READ ENGLISH WELL

The person who has signed above, _____, does not read English well, I read English well and am fluent in (name of the language) _____, a language the subject understands well. I have translated for the subject the entire content of this form. To the best of my knowledge, the participant understands the content of this form and has had an opportunity to ask questions regarding the consent form and the study, and these

questions have been answered to the complete satisfaction of the participant (his/her parent/legal guardian).

Reader/Translator Name:_____

Signature:_____

Date:_____

SIGNATURE OF INVESTIGATOR OR RESPONSIBLE INDIVIDUAL

To the best of my knowledge, the participant, _____, has understood the entire content of the above consent form, and comprehends the study. The participants and those of his/her parent/legal guardian have been accurately answered to his/her/their complete satisfaction.

Investigator's Name:_____ Signature:_____

Date:_____

APPENDIX D RQ1-TRAINING SHEET

1. The Self-test program is meant to test your grasp of world trivia questions.

2. The program will present world trivia questions once you press the next question button

3. Please type T if the statement is true or F if the statement is false into the answer field.

4. You will then confirm by typing your PIN (assigned by the researcher)

5. The program will instantaneously give a feedback on whether your answer is correct or incorrect as well as the cumulative score.

6. The goal is to score the highest in the shortest time.

7. The first five questions are for practice and will not count towards the final score.

8. The cumulative score will be reset after the fifth question to zero in readiness for the real quiz questions.

9. You are allowed to practice severally until you are comfortable with the interface and the task.

10. You will then let the interviewer know when you are ready so that the test can begin.

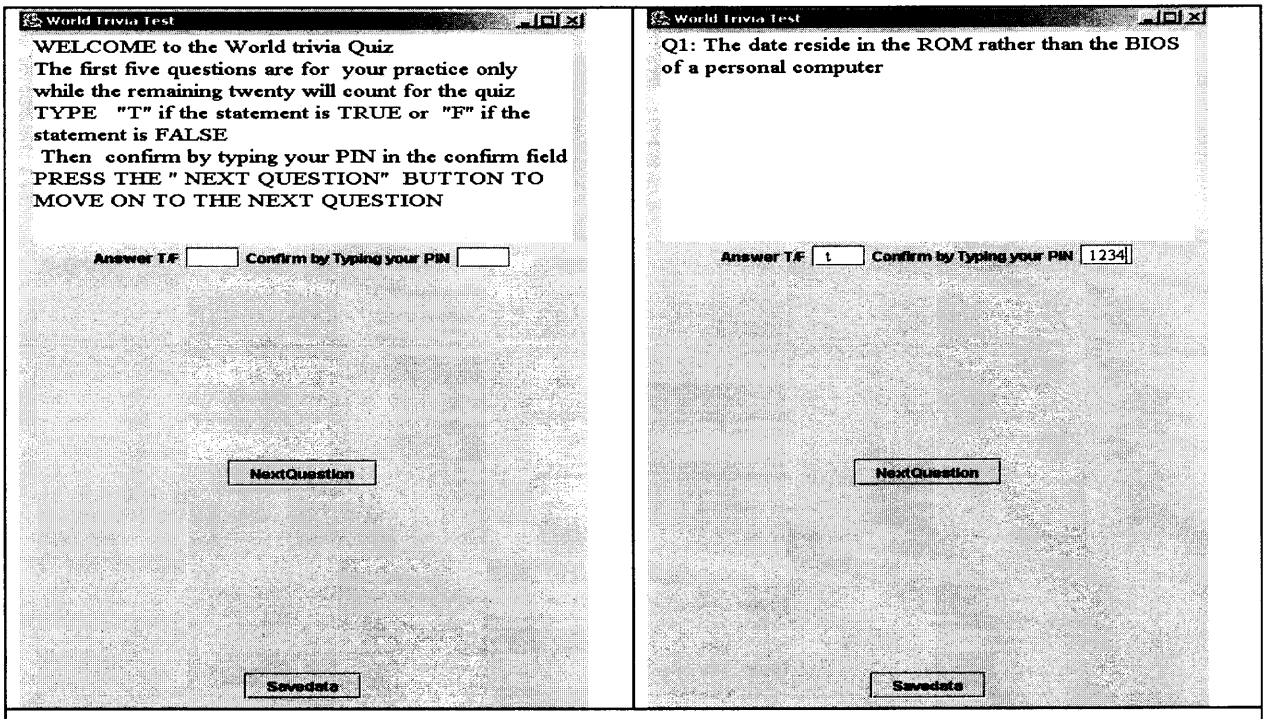

Figure D.1 The world trivia welcome and question screens

APPENDIX E RQ1-TASK SHEET

The world trivia test has 25 questions

The first five questions are for practice and will not count towards the final score

On the fifth question the cumulated score will reset to zero and you will start the actual test

Each question has a single point hence the cumulative maximum score that you can get is 20 points

The objective is to get the highest score in the shortest time

Press the Next question button to start the world trivia self test questions

Please type T if the trivia statement is True else type F

You will then type your PIN (assigned personal identification number) to confirm your answer

Repeat steps 7-8 till you have answered all the questions.

You will get a notification that the quiz is over once you have finished the 25^{th} question.

APPENDIX F RQ2-EXECUTIVES INSTRUCTIONS SHEET

Welcome to the interview

The following are the tasks for the interview

An executive summary on the biometric keyboard will be presented

You will be asked to sign a consent form

You will be interviewed on factors affecting adoption of new technologies

You will be asked to fill in the demographic questionnaire

APPENDIX G RQ2-EXECUTIVES CONSENT FORMS

NEW JERSEY INSTITUTE OF TECHNOLOGY

323 MARTIN LUTHER KING BLVD.

NEWARK, NJ 07102

CONSENT TO PARTICIPATE IN A RESEARCH STUDY

Electronic capture and analysis of fraudulent behavioral patterns: An application to identity fraud

TITLE OF STUDY:

RESEARCH STUDY:

I,_____, have been asked to participate in a research study under the direction of Dr(s). ____Benjamin Ngugi ___

Other professional persons who work with them as study staff may assist to act for them.

PURPOSE: The purpose of this interview is to better understand the critical factors that determines the adoption of new technologies with a specific emphasis on new biometric technologies

DURATION:

My participation in this study will last for one hour

PROCEDURES:

I have been told that, during the course of this study, the following will occur:

An executive summary on the biometric keyboard will be presentedI will be asked to sign a consent form

I will be interviewed on factors affecting adoption on new technologies

PARTICIPANTS:

I will be one of about _____15___participants in this trial.

EXCLUSIONS:

I will inform the researcher if any of the following apply to me:

- I do not wish to participate in the interview and no questions will be asked

RISK/DISCOMFORTS:

I have been told that the study described above may involve the following risks and/or discomforts:

There are no known risks or any anticipated risks

There also may be risks and discomforts that are not yet known.

I fully recognize that there are risks that I may be exposed to by volunteering in this study which are inherent in participating in any study; I understand that I am not covered by NJIT's insurance policy for any injury or loss I might sustain in the course of participating in the study.

CONFIDENTIALITY:

Every effort will be made to maintain the confidentiality of my study records. Officials of NJIT will be allowed to inspect sections of my research records related to this study. If the findings from the study are published, I will not be identified by name. My identity will remain confidential unless law requires disclosure.

Attitude towards biometric ATM questionnaire

PAYMENT FOR PARTICIPATION:

I have been told that there will be NO monetary compensation for my participation in this study.

RIGHT TO REFUSE OR WITHDRAW:

I understand that my participation is voluntary and I may refuse to participate, or may discontinue my participation at any time with no adverse consequence. I also understand that the investigator has the right to withdraw me from the study at any time.

INDIVIDUAL TO CONTACT:

If I have any questions about my treatment or research procedures that I discuss them with the principal investigator. If I have any addition questions about my rights as a research subject, I may contact:

Dawn Hall Apgar, PhD Chair, IRB (973) 642-7616

SIGNATURE OF PARTICIPANT

I have read this entire form, or it has been read to me, and I understand it completely. All of my questions regarding this form or this study have been answered to my complete satisfaction. I agree to participate in this research study.

Subject Name:_____ Signature:_____

Date:_____

SIGNATURE OF READER/TRANSLATOR IF THE PARTICIPANT DOES NOT READ ENGLISH WELL

The person who has signed above, _____, does not read English well, I read English well and am fluent in (name of the language) _____, a language the subject understands well.

Attitude towards biometric ATM questionnaire

I have translated for the subject the entire content of this form. To the best of my knowledge, the participant understands the content of this form and has had an opportunity to ask questions regarding the consent form and the study, and these questions have been answered to the complete satisfaction of the participant (his/her parent/legal guardian).

Reader/Translator Name:_____

Signature:_____

Date:_____

SIGNATURE OF INVESTIGATOR OR RESPONSIBLE INDIVIDUAL

To the best of my knowledge, the participant, _____, has understood the entire content of the above consent form, and comprehends the study. The participants and those of his/her parent/legal guardian have been accurately answered to his/her/their complete satisfaction.

Investigator's Name:_____ Signature:_____

Date:_____

APPENDIX H RQ2-EXECUTIVE SUMMARY FOR BIOMETRIC KEYBOARD

Dear Sir /Madam

I am developing a tool for my doctoral dissertation to transparently mitigate identity fraud at the human computer interface. I hope to benefit from your experience to chart the way forward. Specifically I would like to schedule an interview with you to discuss critical adoption factors that determine the adoption of new technologies and strategic paths that can be used to ensure success. Please let us know of the most convenient time for you. The period should take about an hour. Attached is an executive summary of the research.

Yours faithfully

Benjamin K. Ngugi

Information Systems Department

New Jersey Institute of Technology

University Heights, Newark, NJ, 07102

Office: Tel-973.596. 5422 Cell: 973.280.1205

Email: **benjamin.ngugi@njit.edu**

Dissertation advisors

Michael Recce Co-Chair

Marilyn Tremaine Co-Chair

New Jersey Institute of Technology

Executive summary

Identity fraud has reached alarming proportions and if left unchecked, it has the potential of undoing most of the gains that have emanated from modern technology. The growth of information technology has increased convenience of conducting life management tasks. It is now possible to pay bills, order products and manage our lives from the convenience of our offices or homes. However nothing is without costs. With growth in technology there is a corresponding proliferation of personal information databases, increased uncertainty of the authenticity across a computer network and increased cases of identity fraud. Identity theft is now the leading fraud for the third year in a row affecting more than 27 million Americans. In 2002, losses were $50 billion for individuals and $279 billion for businesses. The fraud continues to rise on a rapid pace.

We are developing a product that can be used to transparently mitigate identity fraud and security intrusions at the human computer interface. An in-depth analysis was performed on the cause of the growth in identity fraud. While there are several ways in which identity fraud can be countered, authentication is the most critical and it can be addressed using appropriate technology. One major problem with current authentication systems is that they use external identifiers like tokens, passwords, and PIN codes. An impostor who has the external identifier is indistinguishable from the genuine owner. Biometrics have the potential to identify the user independent of any other technology but the password and knowledge-based systems are so entrenched that

this may not happen in the near future. An interim solution is to combine the external identifier with a biometric. Most cases of identity fraud and security intrusion occur at a keypad or a keyboard. Extra security at the keypad controls the central point of compromise in identity theft and this security is technologically available.

Several biometric techniques have been considered as a means for protecting from identity theft. These include physical biometrics like fingerprint verification, retina scan, iris scan, face recognition, and hand geometry. They also include behavioral biometrics like speech analysis and handwritten signature verification. In general physical biometric methods are more developed but they require, often expensive, extra equipment and they can be copied. Behavioral biometrics like speech analysis and handwritten signature verification are less precise and they require the user to perform distinct tasks in order to obtain access. The equipment required for behavioral biometrics can also be expensive. Our proposed method, using pressure and time dynamics of typing, is simple, cheap, convenient and transparent to the user.

Prototype development status

We have developed a working prototype that captures the time and pressure patterns during typing and extracts important features using wavelet analysis. The features are then fed into a neural network classifier. We have been able to achieve good discrimination between users in a pilot study.

We need your insights

There is a real gap between proof of concept and successful product. We hope to benefit from your experience to chart the way forward. Specifically I would like to

Attitude towards biometric ATM questionnaire

schedule an interview with you to discuss critical adoption factors that a product similar to our prototype must satisfy if it is to succeed in mitigating identity fraud. Further we are interested in discussing some of the strategic development paths that such a product needs to follow in order to ensure success. We will gladly provide you with a complete report describing our findings.

Possible Business Models for Keyboard Dynamics Authentication

ATM machine integration providing transparent second layer of authentication. Introduce through partnership or license with ATM machine manufacturer.

Entry keypad for high security (e.g. Military or airport security) applications.

(1) Develop through partnership with keypad manufacturer.

(2) Obtain military development grant.

(3) Deploy a purpose-built system to a high security location.

Public freeware release of software to authenticate web traffic using keypad identification.

Revenue through value-added services or charge for higher performance versions.

Each of these potential business models requires distinct product development paths. Our goal is to study the process of product introduction – evaluating the idea that markets should be understood before product development starts. Your assistance in this process is greatly appreciated.

Attitude towards biometric ATM questionnaire

APPENDIX I RQ2-EXECUTIVES INTERVIEW SCRIPT

Researcher: - Briefly summarize the keyboard-based authentication prototype work as per the executive summary

My name is Benjamin Ngugi- PhD. student at NJIT

I am developing a tool for my doctoral dissertation to transparently mitigate identity fraud at the human computer interface.

Identity theft continues on the rise due to several unresolved reasons- expand with focus on Authentication

Have developed a tool that use both time and pressure patterns- achieved reasonable discrimination.

Need to consider business feasibility- critical factors / strategic paths

Would like to learn from your experience introduction and adoption of new (biometrics) technologies similar to such a tool

Give Roadmap

Focus on generic introduction and adoption of new technologies with an emphasis on biometric products wherever possible

Will start with inquiry on background experience

Discussion and ranking of critical introduction and adoption factors for new technologies/biometrics

Critique a tentative model

Evaluate prototype

Evaluate strategic paths/niches

Get some demographic details

Expect to use one hour

Request CIO to give a brief summary of his /her experience and lesson learnt (positive& negative) from introduction and adoption of new (biometric) technologies.

Consider the successful adoptions that you have experienced; i.e. adoptions that were deployed and succeeded in attaining desired goals-what do you think were the critical factors that made these adoptions successful?

Consider the unsuccessful adoptions that you have experienced; i.e. adoptions that were deployed but were either not adopted or failed to work effectively hence later dropped-what were the critical inhibitors (factors) that made these adoption failures?

Are there any other factors not mentioned above factors that would determine the successful adoption of a Biometric innovation like the keyboard authenticator?

Attitude towards biometric ATM questionnaire

Below are some of the factors that we have extracted from literature.

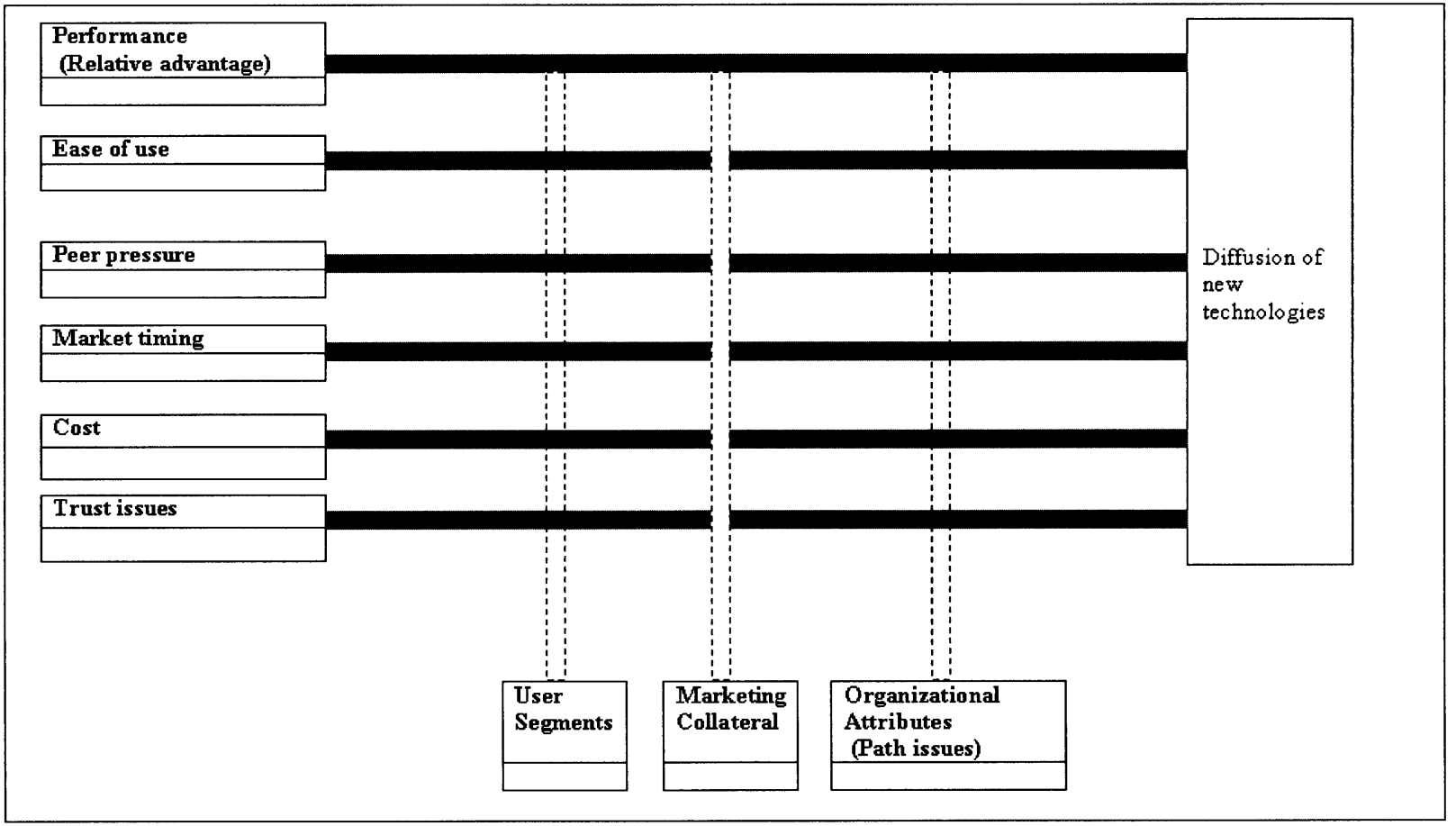

Figure I.1 Preliminary biometric acceptance model

What factors did we miss that are important?

Please rank the aggregated factors in order of importance with respect to adoption of Keyboard tool? Expand on your ranking.

Table I.1 Factors Ranking

Critical factor	Ranking	Justification for ranking
Performance		
Ease of use		
Peer pressure		
Market timing		
Cost		
Trust		

(a) Researcher to elaborate how keystrokes-based authentication works(pressure and time patterns)

(b) What is your opinion of the keyboard-based authentication concept?

How would you compare the keyboard-based authentication to other authentication products (fingerprint verification, Iris recognition, face recognition, voice recognition, password use, smart cards etc) along the dimensions given in the earlier framework replicated below.

Table I.2 Factors Comparison

Critical factor	Comparison with other biometrics like finger print identification
Performance	
Ease of use	
Peer pressure	
Market timing	
Cost	
Trust issues	

What in your opinion are the strengths of the product that can be leveraged along the framework dimensions?

Table I.3 Biometric Strengths	
Critical factor	Strengths of biometric keyboard
Performance	
Ease of use	
Peer pressure	
Market timing	
Cost	
Trust issues	

What are the issues of the product that need to be improved along the framework dimensions?

Table I.4 Biometric Issues	
Critical factor	Issues on of biometric keyboard that need improvement
Performance	
Ease of use	
Peer pressure	
Market timing	
Cost	
Trust issues	

Below are some strategic introductory paths that we think can be used in introducing such products and overcoming the mentioned adoption factors?

ATM machine integration providing transparent second layer of authentication. Introduce through partnership or license with ATM machine manufacturer.

Entry keypad for high security (e.g.. Military or airport) application. (1) Develop through partnership with keypad manufacturer. (2) Obtain military development grant. (3) Deploy a purpose-built system to a high security location.

Public freeware release of software to authenticate web traffic using keypad identification. Revenue through value-added services or charge for higher performance versions.

Each of these potential business models requires distinct product development paths. Our goal is to study the process of product introduction – evaluating the idea that markets should be understood before product development starts. Your assistance in this process is greatly appreciated.

Can you suggest other strategies that we may have missed?

What would be the best three strategies from the aggregated list for introducing such a product? Expand on choice.

What other niche market can we target?

APPENDIX J RQ2-EXECUTIVES DEMOGRAPHIC DETAILS

Age: ☐

Gender: ☐ M ☐ F

Experience with new technologies in ☐

Job Title: _____

Education: ☐ High School ☐ College ☐ Graduate School

The following categories relate to personal characteristics regarding the adoption of new technology.

Please select the category that most applies to you and place an X in the box to the left.

☐ You buy into a new product's concepts very early in its life cycle. You find it easy to imagine, understand and appreciate the benefits of a new technology and base buying decisions upon this belief. You do not base these buying decisions on well-established references, preferring instead to rely on your own intuition and vision.

☐ You share some of the previous category's ability to relate to technology but are ultimately driven by a strong sense of practicality. You know that many newfangled inventions end up as passing fads, so you are content to wait and see how other people are making out before you buy in yourself. You want to see well-established references before investing substantially.

☐ You do not buy unless comfortable with your ability to use the technology. As a result, you wait until something has become an established standard, and even then you want to see lots of support and tend to buy, therefore, from large, well-established companies.

☐ You are very cautious about new technology. You will only purchase when you feel it has become a

APPENDIX K RQ2-USER ACCEPTANCE SURVEY

Questionnaire on user attitudes towards Biometric ATM

Name: _____

Thank you for agreeing to participate in this survey. The questionnaire consist of three parts

Part I-Description of a new keyboard based biometric verifier system at NJIT

Part II- Questions on your acceptance of such a technology

Part II-Questions on acceptable guidelines for such a technology

Answering the questions will take approximately 30 minutes of your time.

Note: All of your answers to these questions will be kept completely confidential. You may at any time, during the completion of this questionnaire decide not to continue.

PART I: THE NEW BIOMETRIC ATM SCENARIO

Fig K.1 Biometric scenario

The information systems department at NJIT is working on new technology that will sense the pressure and time patterns exhibited by a user when typing their personal identification number (PIN). This use of unique behavior patterns to identify a person is called a *biometric* measure. The first application of this biometric technology will be on ATM machines. We will replace the current ATM keypads with new keypads that can detect a person's typing pressure and time patterns. However the new keypads will look and feel exactly like the existing keypads. Likewise the current ATM procedures will be the same. The only difference will be that the user typing pressure and time patterns will be captured and used along with the PIN to verify that the user is indeed the genuine user and not an imposter. This new ATM with biometric technology will hereafter be referred to as the BIOMETRIC ATM'

Pseudo ID: (To be assigned by researcher)

DIRECTIONS: Put an X to the number, which best represents your feelings about each statement in the question that is, how much you agree or disagree with the statement. There are no right answers to these questions. We are asking you to give your own personal feelings and opinions about each of the statements.

PART II-QUESTIONS ON ACCEPTANCE OF A BIOMETRIC TECHNOLOGY

I am worried that a biometric ATM will take too long to verify my identity

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that the biometric typing patterns may be shared with other organizations without my consent.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I believe that no special knowledge or skill is needed to use new biometric ATMs.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

A biometric ATM will be too difficult to use.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

The identity verification on a biometric ATM will require repetition and take too long.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that someone could steal my typing patterns from a biometric ATM.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that the typing training required to use a biometric ATM will take too long.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

1. I intend to use biometric ATMs once they are installed.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

My friends will think that using a biometric ATM is cool (wise).

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I think my typing patterns are so variable that it will be hard for me to learn to use a biometric ATM.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

2. I would avoid using a biometric ATM.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am worried that a biometric ATM will not always recognize me as a valid user.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that someone could copy my typing patterns from a biometric ATM and reuse them to steal money from my account.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I feel that interaction with a biometric ATM will be clear and understandable

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I won't trust a biometric ATM to protect me from identity theft.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Capturing my biometric typing patterns is a serious invasion of my privacy.

0	1	2	3	4
Strongly	Disagree	Neutral	Agree	Strongly

Disagree				Agree

The biometric ATM process of authenticating a user as valid via typing patterns is degrading.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

If I were the first to get a biometric ATM account, I would impress my friends with this information.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

3. I would use a biometric ATM machine if it were conveniently located.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I believe that a biometric ATM will be more likely to prevent thieves from using my ATM card than a standard ATM.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Given the increasing cases of identity fraud, I feel that the time is right to start using the biometric ATMs.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I feel confident that I know how to type in consistent machine-acceptable biometric patterns.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I worry that someone could steal my personal identity from a biometric ATM

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that the collected biometric typing patterns may be used for other purpose like monitoring my activities without my consent.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I believe that it will be harder for thieves to trick a biometric ATM.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am sure that a biometric ATM will have no problems verifying me as the real user.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

My previous experience with computer keyboards and ATM keypads will make the switch to biometric ATMs easy.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I believe that the sole reason the banks are introducing the biometric ATMs is for better protection of my money.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I feel that it will be easy to get the biometric ATM to execute the bank transactions that I usually need

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

4. I worry that a biometric ATM that I don't normally use will not recognize my typing patterns

0	1	2	3	4

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Current ATM systems are secure enough without biometrics.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

The biometric ATM system is an invasion of personal privacy.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I am concerned that I will have a bad day and the biometric ATM will not be able to recognize my typing patterns.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

PART III -QUESTIONS ON ACCEPTABLE GUIDELINES FOR SUCH A TECHNOLOGY

Directions: Fill in the blank in the question with the answer that best descries you

I am willing to pay up to ($_____) for every biometric ATM use if it prevents someone from falsifying and using my card.

0	1	2	3	4
$0.00	$0.10	$0.25	$0.50	$1.00

If you really need cash but were already late for work, how many times would you be willing to retype your PIN number if the biometric ATM had trouble verifying your PIN? (Circle the number, which best applies.)

0	1	2	3	4
Zero more times	One more times	Two more times	Three more times	Greater than three times

If you have nothing scheduled, how many times would you be willing to retype in your PIN number if the biometric ATM had trouble verifying your PIN?

0	1	2	3	4

Zero more times	One more times	Two more times	Three more times	Greater than three times

Imagine you are opening a new bank account. Please circle the number of times you would be willing to type in your PIN number in order for the biometric ATM to learn your unique typing pattern.

0	1	2	3	4
Five times	Ten times	Fifteen times	Twenty times	> Twenty times

How many times in a year, would you be willing to re-train the biometric ATM to update your unique PIN number typing pattern?

0	1	2	3	4
Zero time	One time	Two times	Three times	> Four times

I would not mind going to my bank and repeatedly typing my PIN number for 10 minutes in order to create a unique biometric signature for my PIN number.

0	1	2	3	4
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

User Demographics

Your gender: ___ Male ___ Female

Your Age Group: _____18-25 _____26-33 _____34-41 _____42 and above

Computer usage

Table K.1 Computer Usage				
Computer Activity per week	Less than 10Hrs	10-20 Hrs	>20 and <= 40 Hrs	>40 Hrs
Email				
Programming				
Web Browsing				
Typing				

How often do you use an ATM machine in a week?

☐ Never ☐ Rarely(<1 time) ☐ 1-2 times ☐ 3-4 times

☐ **> 4 times**

For how long have you used an ATM machine?

☐ < 3 Months ☐ 3-12 Months ☐ >1-3 years

☐ > 3 years

You have now finished answering the questions on this questionnaire. Thank you very much for the time and effort you put into responding to these questions. Your answers will help us better conceive of and design security systems to prevent ATM fraud.

APPENDIX L IRB-HUMAN SUBJECTS APPROVAL

NEW JERSEY INSTITUTE OF TECHNOLOGY

Institutional Review Board: HHS FWA 00003246

Notice of Approval

IRB Protocol Number: E20-04

Principal Investigator/Dept: Benjamin K. Ngugi, Information Systems

Title: Electronic Capture and Analysis of Fraudulent Behavioral Patterns: An Application to Identity Fraud

Performance Site(s): NJIT Sponsor Protocol Number (if applicable):

Type of Review: FULL [ ] EXPEDITED [X]

Type of Approval: NEW [X] RENEWAL [ ] MINOR REVISION [ ]

Approval Date: October 12, 2004 Expiration Date: October 11, 2005

ADVERSE EVENTS: Any adverse event(s) or unexpected event(s) that occur in conjunction with this study must be reported to the IRB Office immediately (973) 642-7616.

RENEWAL: Approval is valid until the expiration date on the protocol. You are required to apply to the IRB for a renewal prior to your expiration date for as long as the study is active. Renewal forms will be sent to you; but it is your responsibility to ensure that you receive and submit the renewal in a timely manner.

Consent Form: All subjects must receive a copy of the consent form as submitted. The original signed copies must be kept in a secure place by the principal investigator.

Subjects: Number of subjects approved: 50.

The investigator(s) did not participate in the review, discussion, or vote of this protocol.

APPROVAL IS GRANTED ON THE CONDITION THAT ANY DEVIATION FROM THE PROTOCOL WILL BE SUBMITTED, IN WRITING, TO THE IRB FOR SEPARATE REVIEW AND APPROVAL.

_____ October 11, 2004

Dawn Hall Apgar, PhD, LSW, ACSW, Chair IRB Date

APPENDIX M PSEUDO CODE FOR JAVA PROGRAM

The Java code was about 15 pages long hence will not be put presented in this dissertation due to space. Please find below the main steps.

Read the text file saved from Labview program

Separate the data chunks into different tables each containing data for one PIN digits only which makes four tables

For each of the PIN digits ,determine the first and second trigger voltage by detecting the point that the voltage signal crosses the noise level on the rise and the point where the voltage signal ends

For each of the PIN digits , mark the beginning and end of the voltage pulses

determine the key-down time as the time between the width of this pulse

Superimpose the different PIN digit voltage streams on one frame and determine the inter-key time as the time the end of the first voltage pulse and the beginning of the second voltage pulse.

Store these values into a second set of table.

APPENDIX N- RQ1: TYPING PARAGRAPH FOR TESTING SUBJECTS' SPEED

Introduction by Mr. Pooter

Why should I not publish my diary? I have often seen reminiscences of people I have never heard of, and I fail to see - because I do not happen to be a 'Somebody'

Why my diary should not be interesting. My only regret is that I did not commence it when I was a youth.

Charles Pooter

The Laurels,

Brickfield Terrace

APPENDIX O WORLD TRIVIA QUESTIONS

Table O.1 World Trivia Question for RQ1 Task

This questions were adopted from the World Trivia (Sheppard Software 2004)
for educational purposes only
The original can be found on http://www.sheppardsoftware.com/contst.htm

Q1: The date resides in the ROM rather than the BIOS of a personal computer.
Q2: Netherlands rather than Germany originated the tradition of Santa Claus.
Q3: A person called a Malagasy would live in Madrid rather than in Madagascar.
Q4: United States rather than New Zealand was the first to allow women to vote.
Q5: Daisy-wheel printers could print nice text and full color flowers.
Q6: The Zulu people would be found in Congo forest rather that in South Africa.
Q7: PostScript font standard was developed for the Apple Macintosh but is now universally used for desktop publishing.
Q8: The average thickness of the ice around the perimeter of Antarctica is closer to 3 feet rather 6
Q9: The famous SoHo city section is in New York rather than in London.
Q10: Epson laser printers works by striking pins against an ink ribbon.
Q11: The difference between bubble-jet printers and inkjet printers is because the later use ink.
Q12: The percentage of the Earth's surface that is covered by water is nearer 70% rather than 30%
Q13: Xerox rather than HP was the first to produce LaserJet and DeskJet printers.
Q14: The sun is not visible at the North Pole for 92 rather than 186 days in a year.
Q15: The Nile rather than the Amazon is the only river which flows northward.
Q16: Greece rather than United states was the birthplace of democracy.
Q17: The Year 2000 problem occurred because early programmers used two digits to write dates.
Q18: In 1990, Ethernet rather than HIPPI technology became an official standard for connecting supercomputers and providing high-speed connections for LANs.
Q19: If printed paper rolls up and spits out of your printer before falling to the floor, you've probably got Thermal rather than Laser printer.
Q20: The largest freshwater lake in the world is in Africa rather than in North America.
Q21: The world's most populous democracy is India rather than United States.
Q22: The United states would fit into Africa 2 rather than 3.5 times.
Q23: China rather than United States is the largest consumer of electricity in the world.
Q24: Slave trade from Africa lasted 55 rather than 201 years.
Q25: The name of Apple's first personal digital assistant was Newton rather than palm pilot.

REFERENCES

Aberdeen Group "Identity Theft: A $2 Trillion Criminal Industry in 2005," Aberdeen Group, Boston, MA, 2003.

Albrecht, A. "Understanding Biometrics," Biometrics Today (9), 2002, pp.7-8.

Albrecht, A., Behrens, M., Mansdfield, T., McMeechan, W., Rejman-Green, M., Savastano, M., Statham, P., Schmidt, C., Schouten, B., and Walsh, M. "BioVision: Roadmap for Biometrics in Europe to 2010," PNA-E0303, Probability, Networks and Algorithms, GB Amsterdam, 2003.

Ash, J. "Factors for Information Technology Innovation Diffusion and Infusion in Health Sciences Organizations: A Systems Approach," *Journal of the American Medical Information Association* (4:2) 1997, pp. 102-111.

Australasian Center For Policing Research "The Virtual Horizon: Meeting the Law Enforcement Challenges - Developing an Australian Law Enforcement Strategy for Dealing with Electronic Crime," Report series No.134.1, Australian Center for Policing Research, Adelaide, South Australia, 2000.

Björck, F. "Implementing Information Security Management Systems: An Empirical Study of Critical Success Factors," In: *Advances in Information Security Management and Small Systems Security,* J. Eloff, L. Labuschagne, R. Solms and G. Dhillon (eds.), Klüwer Academic Publisher, Norwell, MA, 2001, pp. 197-211.

Bryan, W.L., and Harter, N. "Studies in Telegraphic Language: The Acquisition of a Hierachy of Habits," *Psychological Review* (6) 1899, pp. 345-375.

Burges, C. "A Tutorial on Support Vector Machines for Pattern Recognition," Data Mining and Knowledge Discovery, Kluwer Academic Series, New York, NY, 1998, pp. 121-167.

Carmines, E.G., and Zeller, R.A. *Reliability and Validity Assessment (Quantitative Applications in the Social Sciences)*, SAGE Publications, Thousand Oaks,CA, 1979.

Cavoukian, A. "Consumer Biometric Applications: A Discussion Paper," Information and Privacy Commissioner, Ontario-Canada, 1999.

Chatelin, Y.M., Esposito, V., and Tenenhaus, M. "State-Of-Art on PLS Path Modeling through the Available Software," HEC Business School, Jouy-en-Josas cedex, France, 2002.

Cheney, J. "Identity Theft: A Pernicious and Costly Fraud," Federal Reserve Bank of Philadelphia, U.S., Philadelphia, PA, 2003.

Churchill, G.A. "A Paradigm for Developing Better Measure of Marketing Constructs," *Journal of Marketing Research* (16:1) 1979, pp. 64-73.

Clarke, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology and People* (7:4) 1994, pp. 6-37.

Conover, W. *Practical Nonparametric Statistics*, (3rd ed.), John Wiley., New York, NY, 1999.

Cortes, C., and Vapnik, V. "Support-Vector Networks," *Machine Learning* (20:3) 1995, pp. 273-297.

Cristianini, N., and Shawe-Taylor, J. *An Introduction to Support Vector Machines and other Kernel-Based Learning Methods*, Cambridge University Press, New York, NY, 2000.

Cronbach, L.J., and Meehl, P.E. "Construct Validity in Psychological Tests," *Psychological Bulletin* (52) 1955, pp. 281-302.

Crossman, E.R.F.W. "A Theory of the Acquisition of Speed-Skill," *Ergonomics* (2) 1959, pp. 153-166.

CyberSource "5th Annual Online Fraud Report," CyberSource Corporation, Mountainview, CA, 2004.

Duda, R., Hart, P., and Stork, D. *Pattern Classification*, John Wiley & Sons, Inc., New York, NY, 2000.

Economics and Domestic Secretariat "Identity Fraud: A Study," United Kingdom Cabinet Office, London, U.K., 2002.

Eger, A., and Blackey, H. "An Investigation into Factors that Affect Adoption and Diffusion of Innovations in Publishing and Librarianship: A Grounded Theory Approach," Proceedings of Canadian Association for Information Science/L'association canadienne des sciences d l'information (CAIS/ACSI), Manitoba, Canada, 2004.

Fornell, C., and Larcker, D.F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Errors," *Journal of Marketing Research* (18) 1981, pp. 39-50.

Fukunaga, K. *Introduction to Statistical Pattern Recognition*, (2nd ed.), Publisher Academic Press Professional, Inc., San Diego, CA, 1990.

Gefen, D., Karahanna, E., and Straub, D. "Trust and TAM in online shopping: An integrated model," *MIS Quarterly* (27:1) 2003, pp. 51-90.

Gentner, D. "Why Nouns are Learned before Verbs: Linguistic Relativity versus Natural Partitioning," In: *Language Development,* S. Kuczaj II (ed.), Earlbaum, Hillsdale, NJ, 1982, pp. 301-334.

Givens, B. "Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions," Privacy Rights Clearing House, San Diego, CA, 2000.

Glaser, B.G., and Straus, A.L. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine de Gruyter, New York, NY, 1967.

Gordon, G., and Willox, N. "Identity Fraud: A Critical National and Global Threat," Economic Crime Institute and LexisNexis, Utica, NY, 2003.

Graeventiz, G. "Biometrics in Access Control," A & S International, Taipei, Taiwan, 2003, pp. 102-104.

Hsu, C.-W., Chang, C.-C., and Lin, C.-J. "A Practical Guide to Support Vector Classification," Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, 2003.

Identity Theft Resource Center Inc. "Identity Theft: The Aftermath 2003," Identity Theft Resource Center Inc., San Diego, CA, 2003.

Jain, A., Prabhakar, S., Hong, L., Ross, A., and Wayman, J. "Biometrics: A Grand Challenge," International Conference on Pattern Recognition, Cambridge, U.K., 2004.

Javelin Strategy and Research "2005 Identity Fraud Survey Report," Javelin Strategy and Research, Pleasanton, California, 2005.

Kotani, K., and Horii, K. "Longitudinal Characteristics of Proprioceptive Memory on Keystrokes: Designing for an Enhanced Authentication System Using Pressures

of Keystroke," 6th International Conference on Work With Display Units (WWDU), Berchtesgaden, Germany, 2002.

Kotler, P. *Market Management*, Prentice Hall, Upper Saddle River, NJ, 2003.

Ma, J., Zhao, Y., and Ahalt, S. *OSU SVM Classifier Matlab Toolbox version 3.00*, 2005.

Malhotra, M., and Groover, V. "An Assessment of Survey Research in POM: From Constructs to Theory," *Journal of Operations Management* (16:4) 1998, pp. 403-423.

Merriam-Webster *Merriam Webster Collegiate Dictionary*, (Eleventh ed.), Merriam-Webster, Springfield, MA, 2003.

Misiti, M., Oppenheim, G., Poggi, J.-M., and Misiti, Y. "Learning About the Wavelet Toolbox 2.2," Mathworks Inc, 2004.

Mohtadi, N. "Development and Validation of the Quality of Life Outcome Measure (Questionnaire) for Chronic Anterior Cruciate Ligament Deficiency," *The American Journal of Sports Medicine* (26:3) 1998, pp. 350-359.

Monrose, F., and Rubin, A. "Keystroke Dynamics as a Biometric for Authentication," *Future Generation Computer Systems: Security on the Web (special issue)* 2000.

Moore, G., and Benbasat, I. "Integrating Diffusion of Innovations and Theory of Reasoned Action Models to Predict Utilization of Information Technology by End-Users," In: *Diffusion and Adoption of Information Technology,* K. Kautz and Pries-Hedge (eds.), Chapman and Hall, London, U.K., 1996, pp. 132-146.

Moore, G.E. "Cramming More Components onto Integrated Circuits," *Electronics* (38) 1965, pp. 114-116.

Mordechai, N., Ido, Y., Ran, E.-Y., and Meir, R. "Towards Behaviometric Security Systems: Learning to Identify a Typist," The 7th European Conference on Principles and Practice of Knowledge Discovery in Databases (ECML/PKDD), Springer-Verlag, Cavtat-Dubrovnik, Croatia, 2003, pp. 363-374.

Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., and Wagner, M. "Keyboard User Verification: Toward an Accurate, Efficient, and Ecologically Valid Algorithm.," *International Journal of Human Computer Studies* (43) 1995, pp. 212-222.

Norman, D., and Rumelhart, D. "Studies of Typing from the LNR Research Group," In: *Cognitive Aspects of Skilled Typing,* W.E. Cooper (ed.), Springer-Verlag, Newyork, NY, 1982.

Nunnally, J.C. *Psychometric Theory*, McGraw-Hill, New York, NY, 1978.

O'Gorman, L. "Securing Business's Front Door- Passwords, Tokens and Authentication," Avaya Labs, Basking Ridge, NJ, 2004, p. 24.

Ord, T., and Furnelli, S.M. "User Authentication for Keypad-Based Devices using Keystroke Analysis," Proceedings of the Second International Network Conference, Plymouth, U.K., 2000, pp. 263-272.

Pandit, N. "The Creation of Theory: A Recent Application of the Grounded Theory Method," *The Qualitative Report* (2:4) 1996.

Pitter, S., and Kamarthi, S. "Feature Extraction from Wavelet Coefficients for Pattern Recognition Tasks," *IEE Transaction on Patterns Analysis and Machine Intelligence* (21:1) 1999.

Polemi, D. "Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, including an Appraisal of the Areas where they

are most Applicable," Report Prepared for European Commission DG XIII-C.4 on the Information Society Technologies, 1997.

Reid, P. *Biometrics for Network Security*, Prentice Hall, Upper Saddle River, NJ, 2004.

Rogers, E. *Diffusion of Innovations*, (Fourth ed.), The Free Press, New York, NY, 1995.

Rosenthal, R., and Rosnow, R. *Essential of Behavioral Research: Methods and Data Analysis*, McGraw Hill, New York, NY, 1991.

RSA Security Inc. "An Enterprise Perspective on Identity Theft," IDT WP 1003, Bedford, MA, 2003.

Shaw, E., Ruby, K., and Post, J. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," Security Awareness Bulletin No. 2-98, U.S. Department of Defense Security Institute, Arlington, VA, 1998.

Sheppard Software *World Trivia Quiz*, Sheppard Software, Jenkintown, PA, 2004.

Smith, R. "Identity Related Economic Crimes: Risks and Countermeasures," *Trends & Issues in Crime and Criminal Justice* (129) 1999.

Synovate "U.S. Federal Trade Commission: Identity Theft Survey Report: September 2003," Washington D.C., 2003.

Templeton, G., Lewis, B., and Snyder, C. "Development of a Measure for the Organizational Learning Construct," *Journal of Management Information Systems* (19:2) 2002, pp. 175-218.

Terzuolo, C., and Viviani, P. "Determinants and Characteristics of Motor Patterns used for Typing," *Neuroscience* (5) 1980, pp. 1085-1103.

Typing Master Finland Inc. *TypingMaster*, Finland, 2002.

U.S. Census Bureau "Home Computers and Internet use in the United States: August 2000," U.S. Census Bureau, 2001.

U.S. Federal Trade Commission "National and State Trends in Fraud & Identity Thefts for Jan-Dec 2003," U.S. Federal Trade Commission, 2004.

U.S. General Accounting Office "Identity Theft: Greater Awareness and use of Existing Data are Needed," U.S. General Accounting Office, Washington D. C, 2002.

Venkatesh, V. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research* (11:4) 2000, pp. 342- 365.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. "User Acceptance of Information Technology: Toward a Unified view," *MIS Quarterly* (27:3) 2003, pp. 425-478.

Whitworth, B., and Zaic, M. "The WOSP Model: Balanced Information Systems Design and Evaluation," *Communications of the Association for Information Systems* (12) 2003.

Yu, J., and Cooper, H. "A Qualitative Review of Research Design Effects on Response Rates to Questionnaires," *Journal of Marketing Research* (36) 1983, pp. 36-44.