# Impact of Perceived Security on Consumer Trust in Online Banking

KRITIKA LAW

A dissertation submitted to the graduate faculty of design and creative technologies
AUT University
in partial fulfilment of the
requirements for the degree of
Master of Computer and Information Sciences

School of Computing and Mathematical Sciences

Auckland, New Zealand
2007

# Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

...........................

Signature

## Acknowledgements

This dissertation was written at the School of Computing and Mathematical Sciences at the Auckland University of Technology.

I would like to take this opportunity to thank all those people who contributed to and made it possible for me to complete this dissertation. First and foremost I would like to thank my supervisor, Dr. Brian Cusack for all his guidance and supervision through the entire study. I would like to express my gratitude to Dr. Cusack for without his encouragement and valuable contribution this research would not have been possible.

To all my lecturers in the MCIS course, I would like to thank them for the guiding me, contributing to my knowledge and honing the skills I required to complete the dissertation.

To my closet friend, Sahil, I take this opportunity to thank you for your support through it all.

I want to thank my parents, Gopal and Pratibha and my brother Manish for giving me the opportunity to continue my education and for all their support, encouragement, love and prayers.

# Abstract

Consumer trust has been recognised as a critical component of the electronic banking industry. Factors that affect trust and its development vary from traditional banking services because of the uncertain nature of the online environment. Extensive efforts in identifying factors that affect trust have shown security to play an important role in its development. Every step in the online banking activities of users are secured by one of more security mechanisms. Analysing the role of these mechanisms in developing a user's perception of security and the impact of this perception on trust provides a pathway to study the role of security in trust development.

The objective in this study is to identify the relationship that exists between trust and security. On analysing prior research, the components of trust and security are identified and these form the basis in defining the nature of the relationship between the two constructs. A model of this relationship is hypothesised based on the theory and empirical results obtained by researchers. This model shows that security for a user exists as a perception and this perception is positively affected by the presence of different security mechanisms. The dimension of trust that is affected by security is institution based trust. Increase in the perception of security is shown to play a positive role in developing this component of trust. These relationships define the connection between trust and security in the e-banking industry.

A survey conducted at the AUT campus provided both reliable and valid data that could further be analysed using confirmatory factor analysis. The results of this analysis show that there is a significant impact of security mechanisms on a user's perception of security  Privacy, authentication, authorization and availability mechanisms are found to contribute the most to the development of their individual perception components and in turn the overall perception of security. This indicated that awareness levels in users regarding security mechanisms of banking websites are high. Thus, these mechanisms play an important and significant role in developing perception of security.

Examining the relationship between perception of security and trust it was noted that perceived security did not have a significant impact on trust. This result shows that the while indicators of security mechanisms had a high impact on perception of security, the perception that they develop does not play a significant role in developing trust. Studying all the individual components of perceived security, it was observed that the perception of privacy did have a significant positive impact on trust. Thus, developing this component of perception would assist the consumer trust building effort for online banking.

# Table of Contents

## List of Tables

## List of Figures

# List of Abbreviations

| | |
|---|---|
| AGFI | Adjusted Goodness of Fit Index |
| ANOVA | Analysis of Variance |
| ATM | Automated Teller Machine |
| AUT | Auckland University of Technology |
| CIA | Confidentiality, Integrity, Availability |
| CFA | Confirmatory Factor Analysis |
| CFI | Comparative Fit Index |
| GFI | Goodness of Fit Index |
| MLE | Maximum Likelihood Estimation |
| NNFI | Non-Normed Fit Index |
| RMSEA | Root Mean Square Error Approximation |
| SEM | Structured Equation Modelling |
| SPSS | Statistical Package for the Social Sciences |
| SSL | Secure Sockets Layer |
| TAM | Technology Acceptance Model |
| TFI | Tucker-Lewis Index |

# Chapter 1
# Introduction

## 1.1 Background

A rapid growth of electronic technologies has transformed the way people transact business. E-commerce application like e-banking, e-tailing and so on have expanded as electronic mediums such as the internet and mobile devices are integrated into daily activities. Electronic banking, like other e-commerce applications, offers an easy to use and convenient medium to conduct banking transactions (Otto & Chung, 2000). Hutchinson & Warren (2003), state that e-banking comprises of more than fifty percent of all banking transaction. These include transactions over all electronic mediums including ATMs, telephones and the internet.

According to Oppliger (1999), the internet in particular has revolutionalised e-commerce. Internet banking has been gaining popularity is the recent years because it provides an accessible, faster and a low-cost method for people to perform their banking activities through a web interface (Claessens et al., 2002). The activities that a user can perform through e-banking include retrieving account information such as transaction history and balance, transferring money between same user's accounts or to different user accounts (Claessens et al., 2002), paying bills (Hertzum et al., 2004), and so on. But, the acceptance of the internet as a tool for banking has been hampered by several concerns.

One of the biggest challenges facing the industry, like most other e-commerce industries is the lack of trust in their customers (Nilsson et al., 2005). Herrmann & Herrmann (2004) find that trust is an important ingredient to accelerate the growth of online applications. The internet based transactions are characterised by uncertainty, anonymity and provides opportunities for people to take undue advantage of the system (Grabner-Krautera & Kaluscha, 2003). The uncertain and unreliable nature of the underlying network would make trust an important element in this environment. Perception of risk within the online environment tends to be higher than most other electronic platforms such as the mobile environment (Suh & Han, 2003).

Understanding the nature of consumer trust and the factors that affect it provides vital clues for its development. Associated with the website, there are several features that are used to build trust, including design, navigation, content, security, usability and so on. Security mechanisms used by websites are noted as one of the most important features that influence consumer trust (Patton, 2004). Yousafzai et al. (2005), find that trust in a physical banking scenario is highly dependent on security and privacy for the consumer. Thus, in virtual banking, the role of security and privacy becomes crucial for building trust.

Security of customer/merchant information is another major challenge facing the electronic commerce industry (Suh & Han, 2003). Ally & Toleman (2005), say that security issues and concerns are raised by customers more often than usability, functionality or other factors when dealing with virtual services. Security of information is often cited as being the single most important concern for businesses and consumers in e-commerce and its related activities (Hutchinson & Warren, 2003). The acceptance of internet as method of banking is often hindered by these concerns of both current and potential users (Yousafzai et al., 2005).

The underlying network (the internet) is considered to be an unsecured medium and applications built on top of this are affected by the same weaknesses in security (Suh & Han, 2003). Patton (2004), explains that the use of internet for commerce has resulted in an open, flexible network over which greater number of functions can be offered to users, but this has also increased the vulnerabilities that could lead to reduced security in such systems. Internet banking is built on public networks would make more susceptible to security breeches. Consumers have more faith in other relatively new networks such as mobile networks in spite of comparatively weaker security.

Resolving the issues of security and trust in e-banking has been undertaken by the industry and the academia. But, due to the vast nature of these issues in online banking and other e-commerce applications, there is still a need for research and development in these fields.

## 1.2 Motivation

The importance of both trust and security in electronic commerce is widely acknowledged in literature (Ally & Toleman, 2005; Yousafzai et al., 2005). While these are independent issues for e-banking, trust and security are considered to be interrelated concepts for most electronic applications. In spite of this, in most prior researches, the two are studied separately. Studies concentrating on security such as Ghosh (1998), Hutchinson & Warren (2003) evaluate the strength of security mechanisms and methods for improving security are discussed. But security in terms of its components and technologies is understood by a small percentage of online banking users. The website's features are often used to communicate and educate users on the security technologies being used. In spite of this awareness, evaluating security from a users perspective and the impact of website security features on a users perception are analysed in a limited number of studies such as Ally & Toleman (2005), Suh & Han (2003), Johnston et al. (2003).

McCullagh (1998), Patton (2004) and other related studies research trust in electronic commerce. They focus on identifying both client characteristics and behaviour of users or service provider efforts for developing trust. A majority of these studies deal with identifying all factors, including security that assist in building trust. The importance of using website features to build trust is often used as basis to study the factors that play a significant role in developing trust. As communicating security through website features has also been identified as a medium to develop perceived security, the effect of the same features on the user's perception of security and on trust is not widely explored. In-depth analysis on the relationship between security and trust are part of a small number of studies including Suh & Han (2003), Yousafzai et al. (2005). The nature of the relationship between the two is relatively unexplored, especially in the context of the banking industry.

Lim (2003) found that security, or rather perception of security can either engenders trust, or vice versa, or can be a mediating factor between trust and willingness in a consumer, or together they can build trusting behaviour. These varying interpretations of the relationship have been studied and contested by several researchers, but the essence of the relationship can be still considered a grey area in this field. Another reason for the lack of agreement stems from the complexity of trust and its components which has resulted in difficulties in understanding the factors that have an impact on it. Restricting the definition of trust to be applicable to the environment in which it is studied would provide a greater understanding of it, but it not practiced often in research (McKnight et al., 2002). This dissertation aims are exploring these areas and understanding the relationship between trust and security from a user's perspective, within the e-banking environment.

In the e-commerce world, there are several applications in which consumer trust would play an important role. E-banking and in particular internet banking was chosen as the domain for this research due to that nature of the transactions involved. Suh & Han (2002), explain that concern for e-commerce security is high in applications where extremely sensitive data is involved. Information exchanged with an electronic bank is highly sensitive, hence consumer concerns related to security are high (Suh & Han, 2003). Online banking sites employ a large number of security measures that customers can experience through their interface (Johnston et al., 2003). Thus, this environment is suited for identifying their impact on consumer perceptions of security and the relationship of perception with trust.

The primary objective in this research is to identify the level of impact of security on consumer trust levels within the e-banking environment. This would include identifying the meaning of trust and its components in the electronic environment. Security would be evaluated from a user's point of view that is a user's perception of security would be studied. In relation to perceived security, the role of security mechanisms that are visible to user through the bank's web interface would be studied. To understand the types of mechanisms that are present, they would be categorised based on the security objective they fulfil. This categorization would be beneficial in evaluating the relative importance of mechanisms belonging to different security objectives for a customer and its effect on their perception of security.

The dissertation would contribute to the understanding of the nature of the relationship between security and trust. This information would be valuable for trust building methods which could concentrate on mechanisms that have a greater effect on security perception and trust. While improving overall security is crucial to electronic applications, analysing security based on objectives such as confidentiality, authentication and so on can lead to a better understanding of the objectives which are valued more by users. Chellappa (2002), argues that improving this understanding is important to sustain electronic applications. The outcome of this study is to research the nature of the relationship between security and trust, which are considered to be the two main barriers in electronic banking and other e-commerce applications. As continuous research and development is taking place to improve security and trust building measures for e-commerce, studying their relationship and the impact of security on trust would benefit in improving these efforts.

## 1.3 Structure of Dissertation

The first chapter in this dissertation acquaints the reader with the motivations to study trust and security, and the objectives of this study. In Chapter 2, the e-banking environment, trust and security and discussed through a review of related literature. The definition of trust is constrained within the online banking environment and only elements of trust that have a potential relationship with security are considered. Similarly, security is defined from a consumer's perspective. A model hypothesizing the relationship between security and trust is developed.

Chapter 3 outlines the methodology used to test the model presented in the previous chapter. Methodologies used in similar researches are reviewed and the methodology that is suitable for this research is discussed. Along with this the data requirements and the limitations are presented.

The next chapter reports the results of the analysis of the data collected. Results from the pilot study on the questionnaire are discussed followed by the findings from the actual data collected through the survey. The validity of the hypotheses based on these findings is discussed.

Chapter 5 discusses the findings of this research in relation to other researchers' findings. It also discusses the validity and reliability of the research results.

The last past of the dissertation comprises of the conclusion in Chapter 6 followed by the references and appendix.

# Chapter 2
# Literature Review

## 2.1 Introduction

Some of the most important issues concerning users and banks alike are customer trust and security of e-banking transactions (Nilsson et al., 2005; Yousafzai et al., 2005). These issues are considered to be inter-related and in particular, security has been identified as one of the most important factors that affect trust levels (Lee, 2002). According to Patton (2004), the users of these systems will trust and accept e-banking only if they perceive the system to be secure, hence security plays an important role is inducing trusting feelings. The concerns over the internet as a medium of banking have been hindered by perceived insecurity of this medium (Hutchinson & Warren, 2003; Suh & Han, 2003), in spite of improved methods to secure these online transactions. Thus, the perception of security plays a significant role in trust building in the e-banking environment.

To improve the overall security of the online banking systems, several mechanisms such as passwords, policies and so on., have been implemented (Claessens et al., 2002). Each security mechanism used aims at fulfilling a particular security goal such as confidentiality, integrity, and so on (Ally & Toleman, 2005; Kesh et al., 2002; Maijala, 2004). While complex technological infrastructures and algorithms may be required to implement these mechanisms, for a user the mechanisms need to be visible through the interface to contribute to their perception of security (Johnston et al., 2003). Along with perception, pre-existing knowledge of these mechanisms also affects user awareness of security (Turner et al., 2001). The perception of security is a concept that can be defined by the level of confidence the end user has in the security of the system. Certain mechanisms that achieve a particular goal (such as authentication) are found to play a more important role in defining a perceived security (Nilsson et al., 2005). Thus, to understand security as viewed by a user, the mechanisms need to be reviewed. Their effectiveness in e-banking transactions would be analysed based on their goal and visibility through the user interface (Ally & Toleman, 2005).

The concept of trust is considered to be ambiguous and dependent of the context in which it is used (Egger, 2003; Suh & Han, 2003). Bargh et al. (2002), explain that building trust in an online environment requires new approaches as compared to traditional business environments, due to the impersonal nature of conduct of online transactions. Trust is considered to be multi-dimensional concept (Tan & Sutherland, 2004), and trust building comprises of addressing the factors the hinder each of these dimensions. In particular, McKnight et al., (2002) explain that trust is made of institution-based trust , disposition to trust, trusting belief and trusting intention. Disposition to trust, trusting beleief and intention are dimensions that are based on the characteristics of the parties that are involved in a trusting relationship. McKnight et al., (2002), go on to explain that institution-based trust is that dimension of trust that is affected by the structure of the environment. Thus, from an external point of view, the factors that improve the perception of this structure would elevate the trust levels. Within this dimension falls the perception of security (Tan & Sutherland, 2004; Yousafzai et. al., 2005).

The importance of security awareness in trust building has been identified in several studies using different research approaches. Few researchers such as Ally & Toleman, (2005), Bargh et al, (2002), Belanger et al, (2002) concentrate on exploring the relationship between security and trust but the measure of the impact of security mechanisms on trust is still a relatively unexplored field. To measure the impact it is essential to understand all the components of the relationship between security and consumer trust. To begin with, Section 2.2 reviews the characteristics of the electronic banking environment. In Section 2.3, the concept of trust is studied and its definition within the constraints of this research is developed. Further, Section 2.4 outlines various aspects of e-banking security and their effect on perceived security. Finally, a framework hypothesising the relationship of security and trust is developed (Section 2.5), followed by the conclusion (Section 2.6).

## 2.2 The Electronic Banking Environment

Electronic banking comprises technology enabled banking activities available to a customer through mediums such as the ATMs, websites and so on (Claessens et al., 2002). The characteristics of each environment may differ based on several factors such as the systems, the users and types of transactions. Within this research, electronic banking would refer to only the online banking scenario and factors related to this environment are discussed below.

The first important characteristic of this environment is the medium on which it is built. Claessens et al., (2002), explain that the increase in the usage and popularity of the online banking medium can be attributed to the fact that it is built upon the internet. Users are inclined to using this system for most banking activities because of its convenient and accessible nature. Along with its benefits, as e-banking relies on the internet, the unreliability and the uncertainty associated with it is a major challenge faced by the industry. These characteristics of the internet have introduced issues related to consumer trust (Nilsson et al., 2005), perception of risk and security. These perceptions held by current and potential customers  are a major block in its acceptance (Yousafzai et al., 2005). Suh & Han, (2003), explain that these perceptions are significantly affected by the current view of the internet and even newer and potentially unsecured environments (such as mobile) are perceived as more secured environments.

Majority of the banking activities would involve the use of highly sensitive, personal information about the customers and merchants (Suh & Han, 2003). Security of this information is highly valued and plays a vital role in defining this online banking setting. Managing and protecting this information is also dependent on the nature of the medium (in this case the internet). Thus, the vulnerabilities and the protective capabilities of mechanisms used over the internet define the security of this environment.

The users and transactions involved also form a part of the online banking environment. The users of this system would be current/potential customers of the bank. The activities that may be performed by these customers would include tracking accounting information, checking account transactions and balances, transferring funds between one or more user accounts (to the same or different banks) (Claessens et al., 2002) and so on. Most banking activities that are carried out through physical communication with the bank are provided online.

These factors or components of the e-banking environments assist in characterising the nature and services offered by banks online. Studying the impact of perception of security on consumer trust would be limited within this environment and these characteristics help in analysing the relationship between the two constructs in the further sections.

## 2.3 Defining Trust in E-Banking

“Trust is the foundation of commerce” (Suh & Han, 2003). It plays a crucial role in the development of human related activities across most industries (Grabner-Krautera & Kaluscha, 2003) including the banking industry (Yousafzai et al., 2005). According to Grabner-Krautera & Kaluscha (2003), building and maintaining trust based relationships between service providers and customers, is being recognised as an increasingly important issue by both research academia and the industries themselves. Trust is considered to be a ‘driving force’ behind the development of e-commerce applications (Herrmann & Herrmann, 2004). Its importance arises from the fact that trust is one of the key factor that determines the acceptance and willingness of consumers to engage in transactions, physical and virtual (Bargh et al., 2002). Trust achieves this by bridging the gap between the customer’s uncertainties regarding the services and their actual participation in the activities (Suh & Han, 2003).

Unfortunately, in the electronic world, the meaning of trust and the trust building mechanisms that are applied in the physical banking world need to be revised (Grabner-Krautera & Kaluscha, 2003; Yousafzai et al., 2005). Traditional definitions of trust are developed to be used within the physical world where services are provided directly from one human to another. Yousafzai et al. (2005), explain that in the virtual environment, the absence of this direct interaction changes the basis on which trust is developed. The virtual environment is characterised by higher complexity and there are higher chances of exploitation (Jones et al, 2000). The degree of uncertainty is higher in the virtual banking setting (Grabner-Krautera & Kaluscha, 2003) and therefore trust is a critical component of this environment. This has also been noted by Patton (2004). The common trust building initiatives used in the physical world, such as eye-contact, tone of voice, appearance and behaviour of people and places, are so on (Yousafzai et al., 2005) are no longer valid in the virtual environment. Thus, the development of other factors that would assist in trust development is gaining importance. For the e-commerce world in particular, using features of a website and information regarding the service providers are commonly used methods of increasing the feeling of trust in users.

To understand the features that are likely to affect consumer trust, understanding the concept of trust is essential. In general, trust has been a difficult construct to define (McKnight et al., 2002). Grabner-Krautera & Kaluscha (2003), in their study on prior researches in the area of trust in e-commerce activities have noted that there are several conflicting definitions of trust that arise from inadequate understanding of trust. A definition most commonly cited in e-commerce literature is by Mayer et al.(1995) who define trust as, ‘‘the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party’’. But the generic nature of this definition does not capture the essence of the environment within which the user is operating.

For this study, the meaning of end user trust needs to be redeveloped for the e-banking environment specifically. To establish a definition of end user trust for the e-banking industry a review of the components of trust and its interaction with environment is essential. Thus, the participants of a trusting relationship are studied in Section 2.3.1. An understanding of the properties and dimensions of trust is developed in Sections 2.3.2 and 2.3.3 respectively. On examination of all these factors, the definition of trust for e-banking is presented (Section 2.3.4) and the factors that affect it follow (Section 2.3.5).

### *2.3.1 Participants of a Trusting Relationship*

Trust is said to exist between two parties who are involved in a transaction. This would comprise of the trustor party who is engaged in receiving the services provided by the trustee party (McKnight et al., 1998). In the e-banking industry, the customers receive banking services from the bank making them the trustors and the electronic bank is the trustee in this environment.

### *2.3.2 Properties of Trust*

To further develop an understanding of trust, the characteristics of its nature must be examined. Based on a study by Bargh et al. (2002) there are several properties that need to taken into consideration while defining trust.

First, trust is relative to a given context, that is, its characteristics would not be the same in different circumstances. This implies while trust definitions would differ from one industry to another, it would also differ within the banking industry. Thus, trust differs in the physical and online transaction scenarios. This dictates the need to re-define trust within the boundaries of an e-banking transaction world.

Secondly, trust is directed from a relying party or trustor to a trustee party. Hence, trust is directional.

The third property of trust is that it is measurable. This allows for possibility of measuring any increase or decrease in trust levels in users at different time instances.

Fourthly, trust exits in time and hence can be observed and measured at different instances.

Lastly, trust evolves in time. This evolution can be attributed to various trust building factors. Managing these factors could help in influencing this evolution.

These properties define trust as a dynamic concept that can be reduced or increased as required.

### *2.3.3 Dimensions of Trust*

Trust is conceptualised as a multi-dimensional construct by most researchers (Grabner-Krautera & Kaluscha, 2003). To define trust completely, each dimension must be identified and different researchers have presented a variety of definitions of the dimensions. McKnight et al. (2002) define trust comprising of four dimensions, namely, disposition to trust, institution based trust, trusting belief and trusting intention (McKnight et al., 1998). While other dimensions have been identified by other researchers such as Kee & Knox (1970), Patton (2004), these four dimensions are most commonly used in trust literature as the basis on which trust is defined (Grabner-Krautera & Kaluscha, 2003; Yousafzai et al., 2005). The first dimension is the *Disposition to trust.* This aspect of trust takes into consideration an individual's tendency to have faith or trust others (McKnight et al., 2002).

*Institution based trust* is the second dimension that is developed through the perception of the environment in which trust is being built (McKnight et al., 2002; McKnight et al., 1998). In the case of e-banking the perception of all factors that are part of the online environment affects this type of trust. This dimension is composed of two parts, Structural Assurance and Situation Normality. The perception of the structure of the environment (which includes factors such as security features, mode of communication and so on) falls under the context of structural assurance. Situational normality comprises of the characteristics of the circumstances that enable interactions between parties to be successful (Yousafzai et al., 2005), and factors such as brand name affect this. A combination of the factors from these two categories lead to development of institution based trust.

The third component of trust is *Trusting Belief* which is the based on the perception of the trustee's attributes that are beneficial to the trustor (McKnight et al., 1998). Trust within this dimension is normally characterised by three beliefs, competence, integrity and benevolence (Grabner-Krautera & Kaluscha, 2003; McKnight et al., 2002; Yousafzai et al., 2005). Competence is the characteristic that defines the belief of the user or trustor in the trustee's ability to do what is required for him. Integrity is the belief of the user that the trustee's commitments in providing services are honest, ethical and will be completed. Benevolence is the user's belief that the party providing services is not taking advantage of them and genuinely wants to provide those services. Each of the characteristics of this dimension do not define an aspect of trust but they lay the foundation for and lead to the development of trust (McKnight et al., 2002).

*Trusting intention* is the fourth dimension that defines the user's aim to be ready to depend of the trustee to provide the services requested.

### 2.3.4 Definition of Trust in E-banking

The objective of this research is to identify the relationship between security (a component of the environment) and trust. Therefore, the definition must ensure that only trust components that are likely to be affected by environmental factors such as security are included. Disposition to trust is a trust dimension that has no interaction with the environment and hence is not considered in the definition. Institution based trust is the component that is built based on the structure of the environment, and trust in this research would in most cases solely refer to this dimension.

In addition, trusting belief is also essential to review as the belief and intention are components that are affected by Institution based trust (Yousafzai et al., 2005) and are an integral part of trust in this environment. Figure 2.1, shows the interactions of these three dimensions that are included in this definition.

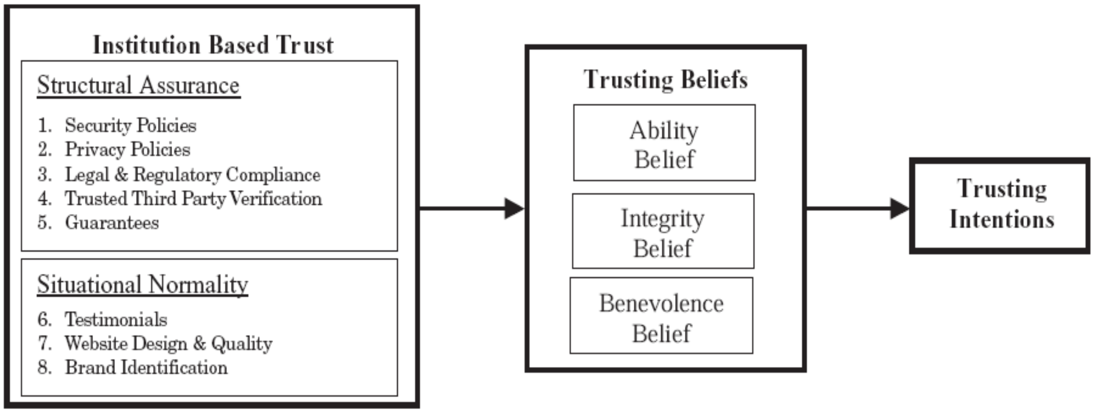

**Figure 2.1 : Trust in Online Banking**

**Source : (Yousafzai et al., 2005)**

On the basis of definition of properties and dimensions of trust, and following the definitions of McKnight et al. (2002) and Yousafzai et al. (2005), trust within the e-banking arena is defined as *" the assured confidence a trustor (i.e., the user) has in the trustee's (i.e., the electronic bank's) ability to provide reliable banking services"*

Comparing this definition to the generic definition by Mayer et al. (1995) can be noted that the traditional meaning of trust where one party relies on another for services and believes they would be fulfilled are still applicable in the online banking environment. In reference to the properties, the definition acknowledges its existence, its environment, and its directional and dynamic nature.

### *2.3.5 Factors that affect trust*

The factors that affect institution based trust are considered in this study. Chellappa (2002) differentiated the factors that affect trust as vendor based and medium based. Vendor based factors are the attributes of the trustee party that are likely to affect trust. This would include brand name, image, marketing strategies and other such factors. Medium based factors are related to the medium of communication, which is the internet for online banking. Using the attributes of the internet to increase consumer trust would involve features such as security and speed of communication.

Belanger et al. (2002) argue that the first factor that assists trust development in online users is the assurance of safety and security. The importance of security in relation to trust is also identified by several other researchers such as (Bargh et al., 2002; Belanger et al., 2002; Lim, 2003). In particular, it is the perception of security, rather than the security mechanisms themselves that affect the level of trust in users of online services (Patton, 2004).

To further develop the nature of the relationship between trust and security, a deeper understanding of security in e-banking is presented in the next section.

## 2.4 Security in E-Banking

Security, being a complex concept, has been defined by several researchers using diverse classification techniques. In general, security is defined as the protection against security threats. In electronic commerce, a threat would be defined as an event that can destroy, modify, waste, deny or disclose information or reduce efficiency of the data and network resources (Belanger et al., 2002). These threats could appear at the client or the server side (Oppliger, 1999) and these could originate due to human, system or communication errors (Bargh et al., 2002). Thus, security assures the protection of the two vulnerable points in e-commerce systems, which are the uncertain underlying technological infrastructure and the unreliable users of the system (Grabner-Krautera & Kaluscha, 2003).

To gain a in depth view of security, in this section a review of the components of security (Section 2.4.1), the meaning and types of security mechanisms (Section 2.4.2) and the interaction of users with these mechanisms (Section 2.4.3) are presented.

### 2.4.1 Components of Security

Security is primarily composed of a set of security primitives or objectives. Each of these objectives aims at protecting the systems and/or users against threats. The primary goals of security are Confidentiality, Integrity and Availability or the 'CIA' triad (Oscarson, 2003). Over time, several other objectives such as authentication and authorization have been identified and been included as an integral part of security. The most widely acknowledged security objectives of e-commerce and its applications are confidentiality, integrity, availability, authentication, authorization, non-repudiation and privacy (Kesh et al., 2002). Hutchinson & Warren, (2003) explain that as Internet banking falls under the spectrum of e-commerce applications they must also fulfil the same set of security requirements. Table 2.1 lists the definitions of these objectives.

Each of the objectives from Table 2.1 covers areas of potential security breeches and attempts to provide a holistic view of the meaning of security in internet banking applications. While some objectives would implicitly imply that other objectives should be fulfilled (for example, confidentiality would require authentication to be achieved) other objectives can be achieved singularly.

**Table 2.1: Security Objectives**

| Objective | Definition |
|---|---|
| Confidentiality | This ensures that the communication between the user/customer and the service provider is not accessible to other parties (Suh & Han, 2003). Unauthorized access of information should be prevented (Knorr & Röhrig, 2000). This should include confidentiality of information that is passed over the network during communication and also the confidentiality of information that is stored at different locations (Maijala, 2004). |
| Integrity | During and after exchange of information, the content should remain unchanged and should be tamper free. This covers both accidental and intentional damage to information data (Grandison & Sloman, 2000). Ally & Toleman (2005), state integrity ensures that messages that are not |

| | |
|---|---|
| | created, modified, interception or deleted by unauthorised people. |
| Availability | The information required by users should be accessible when required by them. This ensures that the system is reliable (Maijala, 2004) and authorized personnel can access the services of an application within a desired time frame (Knorr & Röhrig, 2000). |
| Authentication | Traditionally authentication deals with verification of parties who are communicating to guarantee that they are who they claim to be (Maijala, 2004; Suh & Han, 2003). Claessens et al. (2002), state that authentication must cover both, entity authentication and data authentication. They explain that entity authentication is the verification of the entities or people involved in a transaction. Data authentication is ensuring the data is valid at a particular point in time. |
| Authorization | This objective aims at making sure that the user accessing information has the right to view/manipulate this information (Maijala, 2004). This also includes ensuring that users of e-commerce applications have the permission to send requests and communicate with the system. |
| Non-repudiation | The aim of this is to ensure that the party involved in initiating a transaction, sending any information, or receiving any information cannot deny it at a later instance of time (Maijala, 2004). |
| Privacy | Privacy, though considered by some researchers a separate issue from that of security (Mukherjee & Nath, 2003), has been included by many as part of the security objectives (Nilsson et al., 2005; Patton, 2004). From a customer's perspective, security and privacy may not be discrete concepts, and in most circumstances, security would imply privacy (Suh & Han, 2003). Privacy is defined as the need to guarantee that the customer information is not accessible to unauthorized users and is not misused. |

E-banking transactions normally have a pre-defined set of steps that a user follows to perform the activities. Claessens et al.(2002) explained four steps that defined these activities. Figure 2.2 lists these steps.

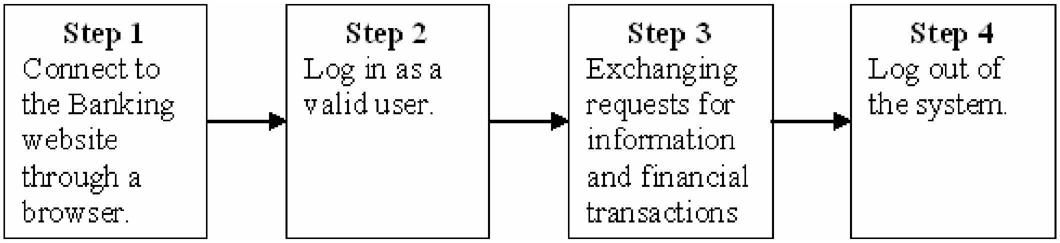
Step 1
Connect to the Banking website through a browser.
Step 2
Log in as a valid user.
Step 3
Exchanging requests for information and financial transactions
Step 4
Log out of the system.

**Figure 2.2: E-banking Activities**

**Based on Classens et al. (2002)**

On analysing each of these steps, the security objectives that were defined above can be mapped to security requirements for user activities. In Step 1, the user should be able to connect to the website within a reasonable period of time, hence dictating the need for the availability objective. Step 2 requires the user's login to be validated and the user should be able to access and manipulate his account information. Thus, authentication and authorization are needed. The third step involves communication of information over a network and therefore, this communication needs confidentiality, integrity and privacy. Through all four steps, the bank customer must be ensured that the transactions requests made by him would be followed through by the bank. This can be ensured by the non-repudiation objective. Thus, security for e-banking applications can be achieved through a combination of these seven objectives.

### *2.4.2 Security Mechanisms*

In an attempt to provide extensive security support for e-commerce applications the objectives defined in Section 2.4.1 must be achieved using different measures. For a user, these measures are means of understanding and interacting with the security of a system. Therefore, in this section a brief overview of the types of security mechanisms used is provided.

Kesh et al.(2002) explain security cannot be defined only as technological measures. There are several mechanisms that are non-technical in nature such as policies, strategies, information listed on websites and so on. All these measures are solutions to countering the threats to the security of the applications and services. Hence, for this paper, security mechanisms are defined as the devices, technologies, methods, measures used to secure a particular system.

Authentication is considered to be one of the most critical security goals that must be achieved for e-banking. Along with that, Hawkins et al. (2000) state that currently most financial institutions including banks employ security mechanisms such as Secure Socket Layers (SSL), encryption of data that is transferred over the internet, digital certificates, etc. To protect customer information stored within their servers, they use firewalls, virus detection and protection methods, backup servers as some of the protective measures.

Table 2.2 shows examples of mechanisms currently employed by the e-banking industry to fulfil various security objectives. Some mechanisms are capable of achieving more than one objective, but their protective capability with respect to each objective may differ.

**Table 2.2: Security Mechanisms in e-banking**

| **Objective** | **Security Mechanisms** |
|---|---|
| Confidentiality | ▪ Cryptography: includes encryption during data transmission and storage (Gollman, 2000; Maijala, 2004; Patton, 2004). |
| Integrity | ▪ Encryption.<br>▪ Digital signatures.<br>▪ Hash functions. |
| Availability | ▪ Back up servers. |
| Authentication | ▪ Passwords (fixed and dynamic) (Claessens et al., 2002)<br>▪ Hardware measures (such as USB tokens)<br>▪ Digital signatures. |
| Authorization | ▪ Access control policies. |
| Non-repudiation | ▪ Digital signatures and certificates |
| Privacy | ▪ Policies and disclosures. |

### *2.4.3 Human Interactions with Security Mechanisms*

The security mechanisms described in the previous section would rely on a complex infrastructure and combination of technologies to achieve their goals. But, for an end user security can only be perceived from mechanisms and they may not truly understand the security of a system. According to Johnston et al. (2003), customers experience these measures through the user interface. They explain that through the user interface a user would be informed about the types of mechanisms used and their protection goals and this would develop their perception. The advances in the protective capabilities of these mechanisms have improved tremendously but in general, customers of online services perceive these to be weak (Suh & Han, 2003). Chellappa (2002) argue that people are less willing to engage in e-commerce services online as compared to mobile services even though they are more secure as they perceive online applications to be more susceptible to threats. Thus, perception of security is a key role in defining a user's view of security.

Perception of security is described as a subjective belief of a user that their communication with the systems is protected from all potential threats (Ally & Toleman, 2005). The security mechanisms act as antecedents of this belief. This can either give the customers confidence to interact with their bank accounts and transact online or can inhibit them from doing so (Ally & Toleman, 2005; Suh & Han, 2003). In Liao & Cheung (2002)'s study, perceived security was rated to be of high importance by users of online banking systems. From a user's perspective, the visibility of these security mechanisms through the user interface is an important aspect and hence the integration of these security mechanisms with the interface is important.

Based on the criteria developed by Johnston et al. (2003), we can study the visibility of different security features. Several features such as user name and password logins, informative error and warning messages, information on the encryption technologies used, symbols such as the padlock sign in browsers are security mechanisms that are visible to users. Each of these conveys the type of the mechanism used to secure the transaction between the user and system. To study the protection offered by an online service, the customers should be made aware of the security goals that are achieved by the website. While it is essential to understand the pros and cons of the mechanisms used in online banking, it  also important to study the indicators of these mechanisms in the user interface which is the first point of interaction between the user and the security measure.

Table 2.3 provides a list of visible security mechanisms for different security objectives that are obtained from review of literature on perceived security mechanisms. While the indicators of security listed in the table do not form an exhaustive list of those used by all banking (and in general e-commerce websites), these are some of the most commonly appearing ones. Other indicators such as security tips provided in the content of a page are all strategies used to improve perception of security.

**Table 2.3: Visible Security Mechanisms**

| **Objective** | **Examples of Visible Mechanisms** |
|---|---|
| Confidentiality | ▪ Padlock Symbol in browser( indicates encrypted connection like SSL) (Hawkins et al., 2000)<br>▪ Warning messages when moving to unsecured network connections.<br>▪ Presence of “https” (Turner et al., 2001). |
| Integrity | ▪ Padlock Symbols (Turner et al., 2001)<br>▪ Warning/Error messages. |
| Availability | ▪ Reduced System Down-time. |
| Authentication | ▪ Login IDs and Passwords (Hawkins et al., 2000). |
| Authorization | ▪ Login pages (Hawkins et al., 2000). |
| Non-repudiation | ▪ Policy disclosure.<br>▪ Padlock symbol indicating page is digitally signed (Turner et al., 2001). |
| Privacy | ▪ Privacy Policy disclosures (Palmer et al., 2001) |

The interaction between customers and security mechanisms will also vary according to the pre-existing knowledge about these mechanisms. In a study conducted by Turner et al. (2001) it was noted that users of online services with fairly advance knowledge of the concepts of security were more aware of the strategies used by different websites to secure their services. These users were convinced about a sites security by the visibility of these features. Based on the previous knowledge of security measures, the users’ definition of good security and the reputation of the site, these users would be guided to look for certain visible security mechanisms that would establish if they found a site secured or unsecured. Unlike these users, the customers with very little knowledge of these mechanisms note visible features and base their opinion of the security of the site on external opinions, site reputation and usability. Hence, this indicates that though security mechanisms can be made visible through various means, the end users would not necessarily observe and interact with them.

Though visible indicators would not always ensure the users understand the presence of security measures, they are the first point of interaction for the users with the mechanisms. Thus, they would have a high potential of affecting the customers perception of security (Johnston et al., 2003; Turner et al., 2001). Hence, this is an important characteristic of the mechanisms that are essential to understand in the context of this study.

## 2.5 Inter-relationship of Security and Trust

In reviewing the concepts of trust and security, security has been identified as a factor that has the potential of affecting trust in an e-banking customer. But the essence of this relationship is still uncertain. To develop an understanding of the relationship between the constructs of trust and security, in this section, a model that hypothesises the nature of this relationship would be developed.

A generic model that outlines the relationship, inferred from the analysis in the previous sections forms the basis of the hypothesis.

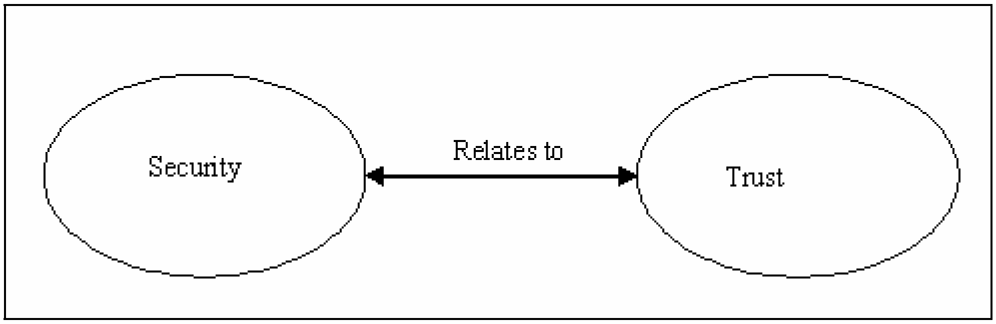

**Figure 2.3: Initial model of trust and security**

Figure 2.3 shows the current layout of the model. The relationship currently states that security and trust are related concepts, but the characteristics of this connection are not defined. Security and trust are both defined as multidimensional concepts (Yousafzai et al., 2005). Therefore, understanding the connection between the different dimensions of these components would assist in analysing the nature of this relationship.

A user may not understand the security provided by mechanisms such as 128 bit encryption algorithm (Suh & Han, 2003). Therefore, for an e-banking customer, security exists as a belief or perception (see Section 2.4.3). The idea of perceived security is a key component that relates to user trust (Chellappa, 2002; Lim, 2003). Visible security mechanisms are considered the antecedent of this perception. Ally &

Toleman (2005), in their study on electronic payment security's effect on consumer trust, developed a framework that identified the relationship between these components of security. In this framework, security composed of mechanisms and user perception together related to trust. Classification of these mechanisms on the basis of security objectives was used as a method of identifying which security mechanisms have a bigger role in developing perception. To evaluate characteristics of the association of security elements, Ally & Toleman (2005), Suh & Han (2003), hypothesised and confirmed that the presence of security mechanisms positively affect the perception of security. Therefore, it can be hypothesised, based on their results, in e-banking too the presence of security mechanisms will positively affect the customer's perception of security.

The next step in the development of the model involves the decomposition of trust. From the definition of trust in this research the components are identified as institution based, trusting belief and intention. Figure 2.4 shows all the components of security and trust that are involved in defining the nature of their relationship.

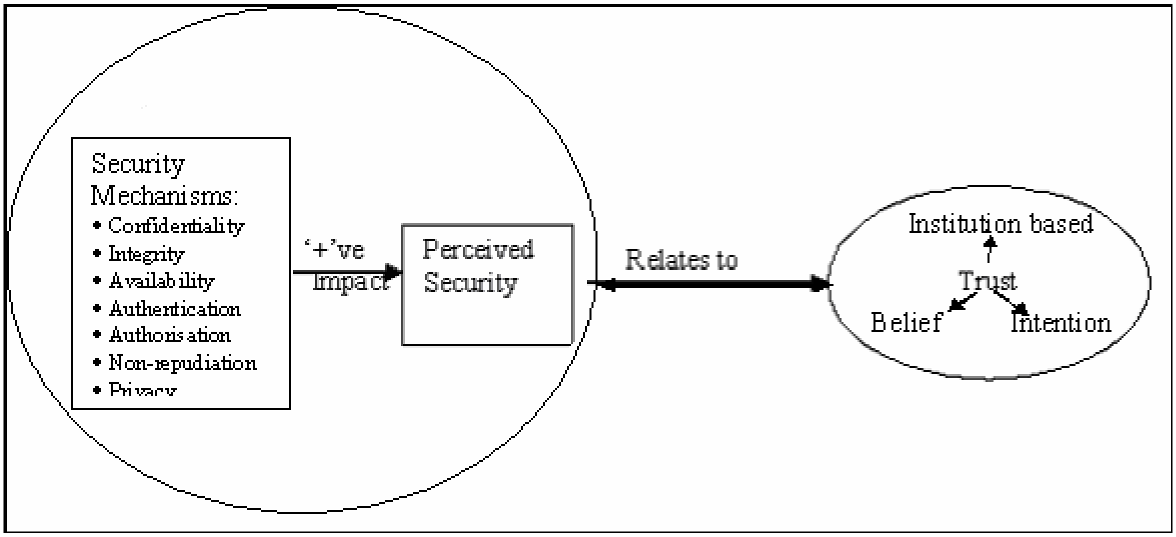

**Figure 2.4: Decomposition of trust and security**

In both Figures 2.3 and 2.4, the direction of the relationship is uncertain. This direction defines if security affects consumer trust or if trust affects security. To further develop directive nature of their relationship, drawing from Lim (2003)'s analysis on perceived risk and trust, four types of relationships are identified. The perception of risk arises from the feeling of uncertainty and the possibility of undesirable consequences arising (Belanger et al., 2002). The perception of security is based on the belief that these risks are minimized. Thus, if perceived risk is high, the perception of security is low and vice versa. Using this relationship between risk and security, Lim (2003)'s definition the relationships perceived risk and trust can be extended to define the correlation between perceived security and trust. On the basis of this, we arrive at the correlations in Figure 2.5.

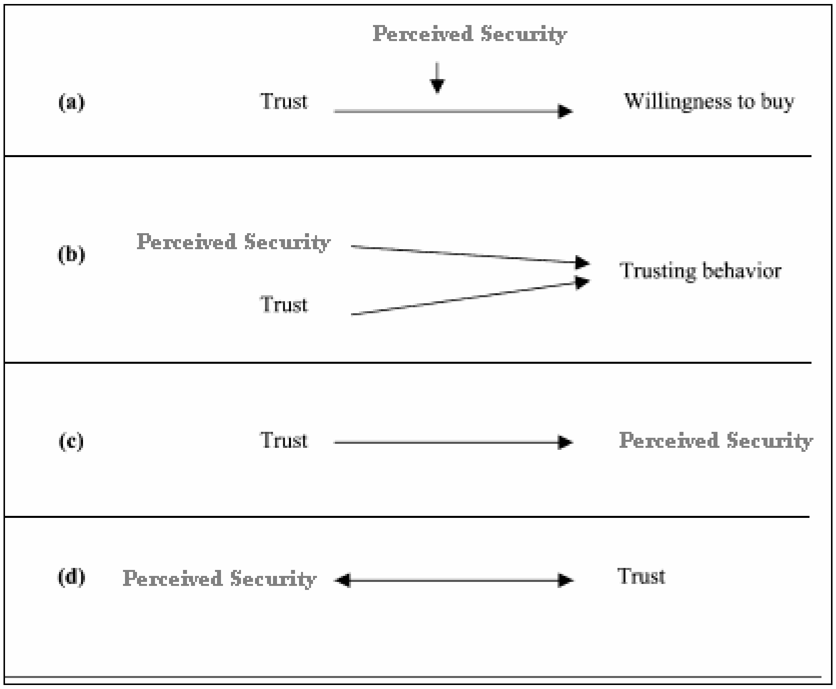

**Figure 2.5: Relationship of perceived security and trust**
**Modified from Lim (2003)**

In Relationship (a), perceived security is a moderating factor that leads customer trust towards willingness to engage in online services. In (b), the combination of perceived security and trust leads to trusting behaviour of customers. (c) explains that trust leads towards the perception of security and (d) expresses that the perceptions of security lead to customer trust.

Each type of correlation asserts the underlying belief held by researchers (Ally & Toleman, 2005; Bargh et al., 2002; Suh & Han, 2003) that trust and security have a symbiotic relationship. Correlation (a) and (b), in addition to trust and security, introduce a third factor, willingness and trusting behaviour respectively. As analysing these concepts are beyond the scope of this research they would not be considered further. Correlation (c) and (d) define opposite directions in which development proceeds. For (c) trust is the antecedent of perceived security and it is vice versa in (d). While, it is argued by many (Bargh et al., 2002; Chellappa, 2002) that security and trust both interact and affect each other, the objective of this research dictates the need to identify security's role affecting trust. In the concept of trust developed in Section 2.3, the dimensions of trust identify perception security as an antecedent for consumer trust. Thus, based on this, the relationship identified in this research is that perceived security leads towards trust.

In Bargh et al. (2002), a framework that studies security and trust in e-business is developed. In their study the placement of security within a model of trust provides a boundary within which security could impact trust. Their framework decomposes trust based on the layer at which it is built. Through their analysis they identify physical trust as the component of trust that is built based on the perception of the physical infrastructure that supports electronic business applications. They consider security mechanisms to be core factors the lead to the development of this layer of trust. Similar to e-business, in e-banking too the same physical infrastructure, i.e., the internet exists. Thus, the mechanisms for security that affect this component of trust would also apply to the e-banking applications. Physical trust is a concept similar to the institution based trust defined by McKnight et al. (2002) and both identify the importance of security in their development.

The effect of perceived security can either positively or negatively affect consumer trust. Empirical evidence gathered in studies by Ally & Toleman (2005), Suh & Han (2003), Chellappa (2002) show that perceived security has the potential of positively affecting trust. Based on their evidence, it can be hypothesised that perceived security positively affect consumer trust in e-banking.

## 2.6 Conclusion

Developing consumer trust in online services is a vital issue that is being extensively studied by the industry and academia. In relation to that, the importance of security as a trust building mechanism has also been identified. Based on these concepts, the value of trust and security in e-banking were discussed in this paper. Trust and security were both identified as multidimensional concepts, and certain dimensions of these were highly interconnected. Institution based trust was identified as the component of trust that could be affected by the security. Similarly, security was defined as a composition of several objectives such as confidentiality, integrity and so on. But, for a user, the belief of security was a crucial component defining their view of security.

Analysing the theory behind these dimensions, security mechanisms, perceived security and trust (institution based) were the three correlated concepts. Building a model of the relationship between trust and security, the hypothesis of the nature of their connection was developed. Firstly, the presence of security mechanisms was hypothesized to have a positive impact on the perception of security. Secondly, the increase in perception of security was said to have increased the level of trust in consumers. Thus, security plays and important role in the development of trust in e-banking customers.

To verify this framework, confirmation of the nature of the relationship using empirical data is carried out. This data comprises of the measurement of the degree or level of impact of perceived security on consumer trust and forms the basis of the verification purposes. In the next chapter, the research methodology, data collection and analysis methods are extensively reviewed and the most suitable methodology and methods are presented.

# Chapter 3

# Research Methodology

## 3.1 Introduction

The Chapter 2 literature review identified a plausible model of trust and security. The next step is to identify the main research questions and a working model that hypothesises the relationship between the two constructs. This model presents the hypothesised relationships between security mechanisms, perceived security and trust, as these were identified as the three components that would be studied within this research framework.

On building the research model the steps to empirically test the model were to be decided. The evaluation and modification of the model was carried out by collecting and analysing information from e-banking users. This information was then used for testing the hypotheses and provided a deeper understanding of the relationship between security and trust. As this research concentrates on the effect of visible security mechanisms on user perception of security, information related to perceived security built for security mechanisms and trust is evaluated.

In this chapter, the model of Chapter 2 is carried forward and prepared for testing. To identify the appropriate research methodology for this study, a review of methodologies used in similar studies is presented in Section 3.2. Based on the analysis of these studies, the research design for this study is developed in Section 3.3. The questions and hypotheses are then presented, followed by a specification of the data requirements for this study (Sections 3.4 and 3.5 respectively). Sections 3.6 and 3.7 discuss the limitations of the methodology and conclusions of this chapter.

## 3.2 Review of Similar Studies

Five studies are now reviewed to observe how other published works have elaborated and explained their preferred methodologies. The first concerns the perception of trust by online customers that was completed with a random sample of students. The second addresses trust and security in the context of the Technology Acceptance Model (TAM). The third study looks at site attributes and the willingness of customers to provide personal information. The fourth links risk to perception and was completed using survey methods. The final study looks at the relationship of security mechanisms and consumer trust.

### *3.2.1 Role of Website Attributes in Trust Development*

In their study on trust development, Yousafzai et al. (2005), aimed at studying trust building strategies and the use of website attributes in developing the perception of trust in online customers. The interrelationship between security, privacy and trust in the banking industry (physical and virtual) was studied as the central concern. The study focused on evaluating the impact of different website attributes on trust levels in consumers. These attributes, identified through the review of prior research, including brand name, content of site, privacy and security policies and mechanisms. Trust in this study also focused on institution based trust, trusting belief and intention. Thus, factors related to the structure of the environment are considered in their study and hypotheses are developed about the relationship between these factors and trust. The presence of different attributes was hypothesised to develop trusting belief in consumers.

To empirically verify their hypotheses, the researchers chose an experimental setting within which a random sample comprising of students participated. A preliminary study of banking websites was carried out by the researchers to select websites which represented maximum coverage of features being studied in relation to trust. Groups of users were asked to navigate these websites. Information related to the impact of website features on their trust was collected through questionnaires. The Likert scale was used to allow participants to select the degree to which they agreed/disagreed to a question. Analysis of this data was carried out using ANOVA to understand the variance between different groups.

Features of the virtual environment were found to play an important role in trust development. In particular, the presence of security, privacy, legal statements and guarantees resulted in a significant increase in consumer trust levels while others such as testimonials contributed only by a small percentage to development of trust.

### *3.2.2 Role of Trust and Security in Banking*

The impact of consumer trust and perception of security on acceptance on technology has been explored by several researchers including Lim, (2003), Slyke et al., (2004). In Suh & Han (2003), a research model based on the Technology Acceptance Model (TAM) was developed to understand how users accepted this technological model. The model included hypotheses, in which acceptance of e-banking was based on identifying the connection between security, trust and actual use. First, the perception of security control is assumed to have a positive impact on trust. Further, trust is hypothesised to have a positive impact on acceptance of and intention to use internet banking. To analyse security in more details, the impact of individual security objectives (such as authentication, integrity, confidentiality) were considered individually in the research model.

To test the model a web based survey was conducted. The survey was made available on a banking website. The electronic questionnaire ensured that the sample was random and comprised of internet banking users. A seven point Likert scale to allow for quantification of answers was used. Measures for trust and acceptance were based on previous research and merged with the current objective. For security, measures were also re-developed based on a literature review. Only the security measures that would be visible to customers were included in the questionnaire. Structured Equation Modelling (SEM) was used to model the data. The SEM model tested causal relationships where multiple measurement items exist.

The perception of security was found to play a significant role in the acceptance of internet baking. In particular, non repudiation, privacy protection and data integrity were the most important from a user’s perspective and had a positive influence on the consumer’s acceptance of this technology.

### *3.2.3 Trust, Privacy and Security Attributes*

The importance of privacy, security and other site attributes within the e-retailing environment and their effect on trust is researched in the paper by Belanger et al. (2002). Four websites attributes that act as trust indices and their effect on trust were evaluated in depth. These included security features and statements, and privacy seals and statements. Also, the extent to these indices affect willingness to provide information was analysed. The relative importance of privacy, security and other features such as ease of use, website design in trust building was also examined. Security features were hypothesised to be of higher importance in consumer trust development as compared to the other three indices. Other hypotheses state that trust would positively affect willingness to provide information and intention to purchase online.

A random sample of university students volunteered to participate in a survey based in an experimental setting to test the hypotheses. This data collection method is similar to the study by Yousafzai et al. (2005). A preliminary study of different websites was carried out to identify the websites to be included in the experiment. Participants answered a questionnaire before and after the navigation through the chosen websites. These questionnaires presented had undergone prior analyses using Cronbach's alpha and factor analysis. The data collected from the experimental survey was analysed using paired comparison t-tests.

The results revealed that security features were comparatively more important than privacy and security seals and statements for developing a consumer's perception of security and trust. In contrast to Suh & Han (2003), the trustworthiness of a site was found to be high even if indices of privacy and security were low; showing that other features such as content layout, design and so on may play a vital role in building trusting perceptions. Other results included the confirmation that trust and willingness to purchase positively influenced purchase intentions.

### *3.2.4 Trust Development using Security and Privacy*

Chellappa (2002)'s study proposes that consumer risk in e-commerce is not only based on perceptions of the vendor but is also influenced by perceptions of risk and security. The roles of perceived privacy and perceived security in engendering trust are studied in this paper. The difference in trust levels in consumers within the online environment and the offline store environments is hypothesised to be significant. This hypothesis is based on the researching prior studies that indicate the perception of privacy and perceptions of security is lower in online rather than offline purchases and improved perceptions of these online lead to increase in trust levels.

A survey was conducted to test the hypotheses. The survey was administered in two parts, the first to a sample of graduate business students and the second with a different set of graduate and under graduate students. Participants were gathered on a voluntary basis and were offered a reward for participating. The first survey aimed at analysing the differences in trust levels between online and offline stores though an online questionnaire. This study also served as a pilot study for validating the measures used for perceived security and privacy. The second study then analysed the correlation between perceived privacy, security and trust. Analysis was carried out using paired t-tests.

The results of their study indicated that perception of security, privacy and trust in online stores is lower than their counterparts in the physical world. Perceived privacy is not found to have a significant improvement on trust and instead is found to be a component of perception of security rather than a separate entity. Perception of security is concluded to play an important role in trust development.

### *3.2.5 Impact of Individual Security Features on Trust*

In Nilsson et al. (2005), a single category of security mechanisms, that is, the authentication mechanisms and their impact on consumer trust is studied. The types of authentication mechanisms that contribute to building trust are examined. Basing their research on studies such as Aladwani (2001), Suh & Han (2003) which identify perceived security as a significant contributor to trust development, Nilsson et al. (2005) study the authentication features that have an impact on perceived control, awareness and trust in e-banking consumers. Two main authentication types were identified for this purpose, fixed passwords and security boxes. Security boxes refer to randomly generated passwords as opposed to pre-defined fixed passwords.

To identify the important authentication measures in e-banking a triangulation of data collection methods were used including interviews and questionnaires. The questionnaire was built using Likert scales to represent the relationship between authentication mechanisms and trust. The sample for the questionnaire consisted of random participants from European countries and had varied experiences with internet banking. To further validate the results of the survey, a small percentage of open questions were included in the questionnaire. In-depth interviews were conducted with users who used different banking websites with different authentication mechanisms. The results of the interviews were analysed using grounded theory and this was used to verify the data for the survey.

Based on the analysis of the data from the survey four important factors were identified related to the two main authentication mechanisms. Trust in online banking was found to be higher in users using banking websites with security box mechanisms. The perception of security related to security boxes was also higher as compared to fixed passwords. Security boxes also gave users more confidence and perception of control over their transactions while accessing their accounts from public locations.

## 3.3 Research Design

The five studies reviewed in the preceding Sections have introduced a range of ways others have researched the relationship of security and trust. A central aspect of this research is to identify the relationship between security and trust in consumers. This involves an assessment of consumer perceptions and trust levels while dealing with the electronic banking medium. The objective of the research is to study the relationship between these two objects by providing empirical evidence for the same. From the review of earlier literature it is seen that a qualitative approach is more suited for empirical verification of the relationship. Section 3.2 reviewed the research methods that were used in related studies. These studies followed a quantitative approach in their research using both qualitative and quantitative data types. Thus this approach was selected for this study.

A variety of methodologies have been used by researchers including surveys (Suh & Han, 2003; Chellappa, 2002; Ally & Toleman), experiments (Yousafzai et al., 2005) and exploratory case studies (Ratnasingham & Kumar, 2000). The case study approach was used mainly while studying trust in e-commerce within the confines of an organization. Based on the analysis of prior researchers,  the case study approach was not found to be suitable to achieve the research objective; this approach was not discussed further. As seen in the previous section, the survey and experimental setting were preferred methods to study trust and security relationships. Considering the time and resource limitations, a survey based approach is chosen over an experimental setup in the research (Collis & Hussey, 2003). A survey based approach is suitable as it helps establish the strength of the relationships and values of the different variables.

The research involves three phases (see Figure 3.1), a review of prior studies, and the administration of a survey and analyses of the results. In the first phase, the analysis of the literature was carried out to determine the measures of perception of security and trust. Using measures from previously published literature has been followed by researchers such as Suh & Han (2003), Chellappa (2002) in their studies on trust and security in electronic mediums. The same approach was followed for the development and administration of the survey. The data collected from the survey was mainly quantitative in nature. The survey focuses on establishing the impact of security mechanisms on perception and on consumer trust. The contribution of perceptions related to different security objectives (such as confidentiality, integrity and so on) were then considered individually. Thus, enabling the research to establish the impact each objective has on trust development.

In the final phase the analyses of the results was carried out. At the end of the analyses, the nature of the relationship between security mechanisms, perception and trust was studied. The analyses of the data also helped in refining the research methods, the measures and the research model developed. This makes the entire process iterative.

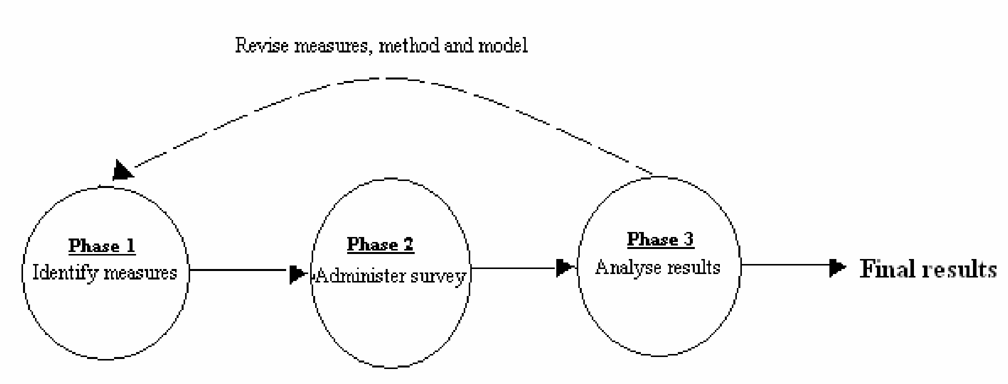

**Figure 3.1 : Research Design**

## 3.4 Research Model

The literature review in Chapter 2 provides a basis on which to assert a set of hypotheses, and to define a research question and sub questions.

The main research question in this study is:

*What is the impact of security on trust?*

From the previous chapter, it can be seen that security is composed of mechanisms and user perception. Based on the hypotheses of the relationship between mechanisms, perception and security we can decompose the main question as follows:

*What is the impact of perceived security on consumer trust in online banking?*

*What is the impact of security mechanisms on perceived security and in turn on trust?*

In Chapter 2, it was noted that security mechanisms positively affect perception of security and perception of security positively affects trust. From this we note that security mechanisms are the independent variables in the relationship while perception and trust are the dependent variables.

The final model capturing this relationship is presented in Figure 3.2.

Based on this model, the relationship between security and strength are based on the relationship between mechanisms and perceived security, and perceived security and trust.

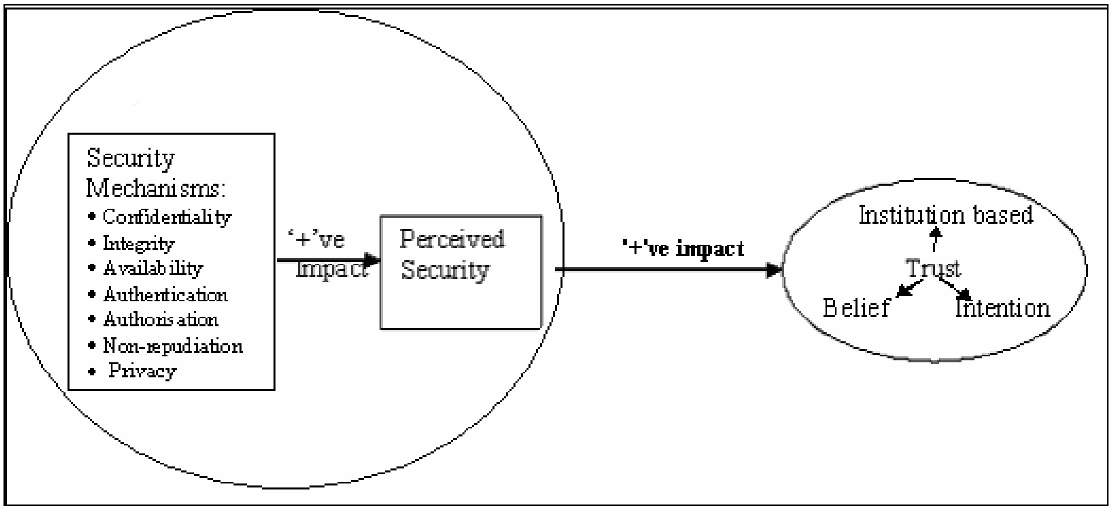

**Figure 3.2 : Final Model for trust and security**

The hypotheses for these relationships are as follows:

> *$H_1$: The presence of security mechanisms positively affects a user's perception of security.*

This hypothesis can be decomposed and developed for each security objective defined as follows:

> *$H_{1a}$: The presence of confidentiality mechanisms positively affects a user's perception of security.*
>
> *$H_{1b}$: The presence of integrity mechanisms positively affects a user's perception of security.*
>
> *$H_{1c}$: The presence of availability mechanisms positively affects a user's perception of security.*
>
> *$H_{1d}$: The presence of authentication mechanisms positively affects a user's perception of security.*
>
> *$H_{1e}$: The presence of authorization mechanisms positively affects a user's perception of security.*
>
> *$H_{1f}$: The presence of non-repudiation mechanisms positively affects a user's perception of security.*
>
> *$H_{1h}$: The presence of privacy mechanisms positively affects a user's perception of security.*

The alternative hypothesis for this would be:

> *$H_0$: The presence of security mechanisms negatively affects a user's perception of security.*

Using these hypotheses, the contribution of different mechanisms to perception and trust can be evaluated. The second hypothesis in the model is:

> *$H_2$: An increase in the perception of security positively affects consumer trust.*

These hypotheses define the relationship between security, its mechanisms, interactions with end users and its effect of their trust.

## 3.5 Data Requirements

To test the hypotheses and research model developed in section 3.4, data is collected and assessed at each stage in the research process. In the first stage, information related to security and trust measures is collected from prior literature. The questionnaire developed based on these measures is tested with a pilot group. Feedback from this pilot group is incorporated in the questionnaire design. Finally, data is collected from the survey and undergoes analyses.

The pilot study is defined in Section 3.5.1 followed by the definition of the sample size, participants and recruitments process in the next section. The data collection methods including the questionnaire design and the methods used to process this data are included in Sections 3.5.3 and 3.5.4 respectively. Lastly, the data analysis techniques are defined in last Section 3.5.5.

### *3.5.1 Pilot Study*

Pilot studies are used by researchers such as Suh & Han (2003), Chellappa, (2002) as a method of reviewing and refining their data collection instrument. The measures chosen from previous studies on trust and security in the online environment could then be revised and adapted according to the goals of this research. A pilot study was conducted to obtain feedback on the questionnaire design and ease of understanding the questions. In the pilot group providing feedback, an effort was made to include 8-12 MCIS post graduate students and lecturers. Based on this feedback the questionnaire was then to be revised before the final survey.

### *3.5.2 Sample*

A random sample of students from a university was chosen for the survey. A sample of students is widely used in research on online trust in studies such as (Jarvenpaa et al., 2000; Gefen 2000 Lee and Turban, 2001; Chellappa and Pavlou, 2002). Random sampling ensures that every user has equal chances on being selected to participate in this study and reduces bias in the sample

Participants were to be recruited on a voluntary basis. They were approached on the AUT Wellesley campus. Randomly approached students were asked if they have prior online banking experience and those with prior experience were selected and invited to fill in the questionnaire. A small incentive, such as a food or beverages, at a cost of no more than $5 was initially included as part of the approach.

The best suited sample size was determined using multivariate techniques such as statistical power analysis. Anderson et al (1998), plotted a graph of power versus sample size for different significance levels (∝ - value). For this study, to obtain a power of 80%, significance level of 0.05%, a sample size of 130 participants is considered ideal based on this graph. These participants consisted of students from AUT. The diversity in the students represents a wide variety of internet banking users, making this a viable sample.

### *3.5.3 Data Collection Methods*

According to Collis & Hussey (2003), questionnaires are considered to be suitable data collection methods in surveys that involve a relatively large sample. Questionnaires are used to collect information in similar studies listed in section 3.2 and Suh & Han (2002), Lee and Turban (2001), Chellappa and Pavlou (2002). The questions were categorised according to the security objective they refer to, thus preventing the participants from getting confused, missing questions and other such issues (Dillman, 2000).

To measure the perception of security and trust the items developed in the questionnaire were to be adapted from previous studies including Suh & Han (2003), Yousafzai et al. (2005). The questionnaire and items were then modified based on the feedback from a pilot study group.

The questionnaire consisted of closed questions and no personal questions would be included. The answers for the question set were represented by the Likert scale, allowing to respondents to select the level of impact the objectives referred to had on their trust (Collis & Hussey, 2003). This enabled scoring the replies and quantification of the research findings (Dawis, 1987). The Likert Scale was also preferred in the studies reviewed in Section 3.2.

The questionaire was composed of two main sections for perception of security and trust respectively. The first section includes measures of the perception of confidentiality, integrity, availability, authentication, authorization, privacy and non-repudiation based on visible security mechanisms. Measures for trust, which include measures for institution-based trust, trusting belief and intention form the next section. (Refer to Appendix B)

### *3.5.4 Data Processing Methods*

A paper-based questionnaire was then to be distributed for the participants to fill in. It was estimated that they needed between 5 to 10 minutes to complete this survey, during which no personal information was collected. A collection box was to be used for participants to deposit their questionnaires.

The data was then coded and transferred to a SPSS package for statistical analysis of the data. The analysis packages are capable of handling incomplete questionnaires based on the percentage of missing data. Measures with a large percentage of missing data was omitted from the analysis as drawing results based on the information would be biased and incomplete.

### *3.5.5 Data Analysis Methods*

The first phase of analysis includes a review a prior research to identify items for the measurement of trust and security. These items are adapted to suit this research and included in the questionnaire. The measures for perception of security are based on the visible security mechanisms for the seven security objectives, as discussed by Hawkins et al.(2000), Turner et al. (2001), Suh & Han (2003), Palmer et al. (2001) (See Appendix B, Section two). The measures for trust were adapted from studies including Suh & Han (2003), Chellappa (2002). The feedback from the pilot study was then used to modify the items for measurement and the design of the questionnaire.

The data collected from the survey was analysed using statistical analysis methods. Statistical analysis techniques have been widely used while studying trust relationships in electronic applications (Grabner-Krautera & Kaluscha, 2003; M.K. & lee, 2001; Suh & Han, 2003). Related studies such as Yousafzai et al. (2005), Belanger et al. (2002) use analysis techniques such as ANOVA, paired t-tests, SEM and so on. Techniques such as ANOVA and paired t-test were used in researches where data is collected in an experimental setting from multiple user groups and therefore are not considered in this study. Structured equation modelling enables generalised conclusions to be drawn about a population from a smaller representative sample and is used to test relationships based on hypotheses (Collis & Hussey, 2003). Thus, SEM was chosen as the analysis method for this study.

SPSS packages such as LISREL or AMOS were used in this phase. The first step of analysis included the creation of a path diagram of the research model. The correlation matrix was used as opposed to the variance-covariance matrix the input matrix for analysis as this is suitable when a single sample is used in study (Suh & Han, 2003). The validity and reliability of the measurement items of security and trust were tested using Cronbach's alpha and Confirmatory Factor Analysis which are widely used for this purpose (Belanger et al., 2002; Yousafzai et al., 2005). The Assessment of Fit of the model was also carried out to analyse how well the data fits the given path model.

Figure 3.3 shows the mapping of the research questions to the research phases in which they were analysed. The data collection instrument for each phase and in turn the questions they answer are linked. Finally, the hypotheses that this research is based on were mapped to the questionnaire items that were be used to test them.

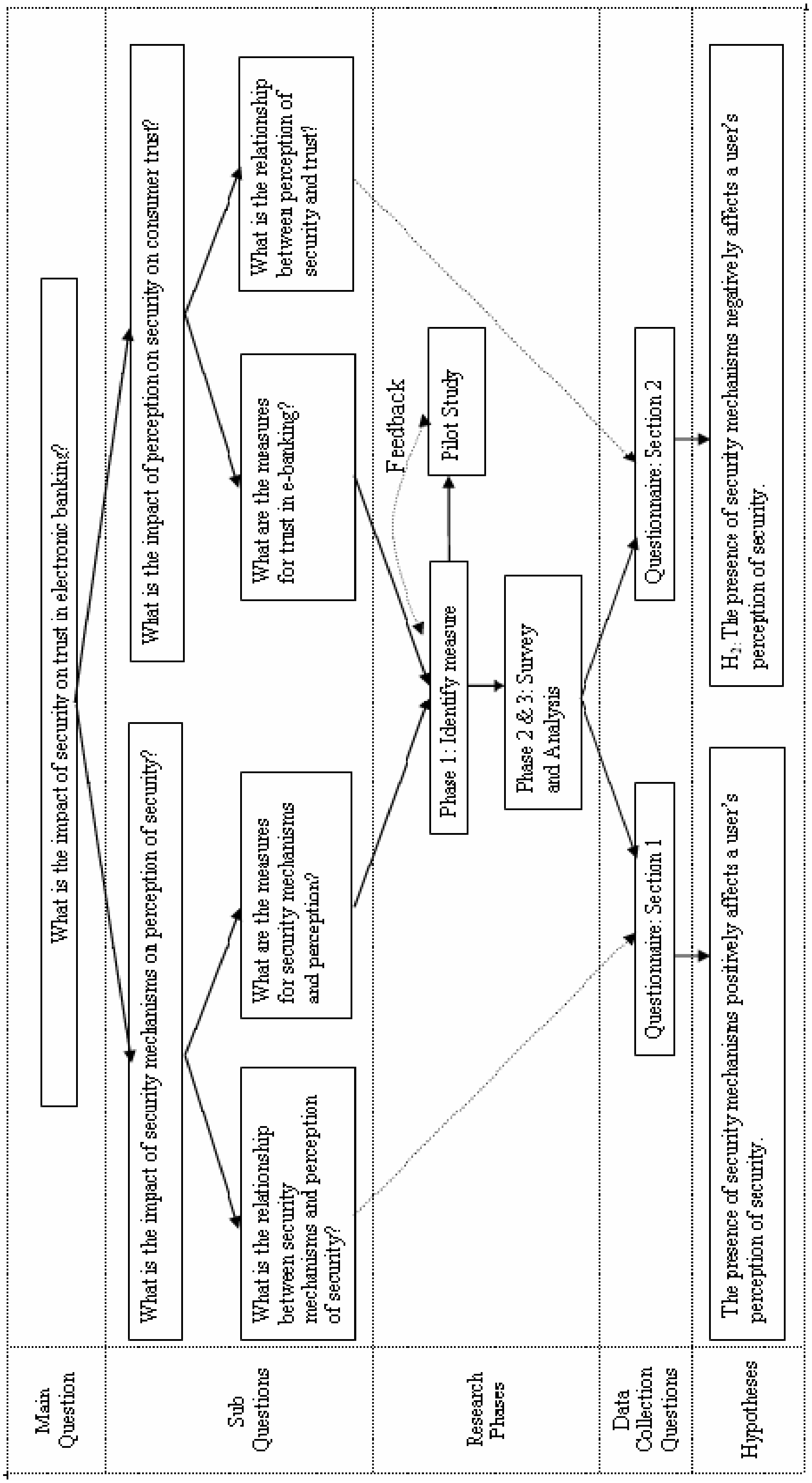
Main Question
Sub Questions
Research Phases
Data Collection Questions
Hypotheses
What is the impact of security on trust in electronic banking?
What is the impact of security mechanisms on perception of security?
What is the impact of perception on security on consumer trust?
What is the relationship between security mechanisms and perception of security?
What are the measures for security mechanisms and perception?
What are the measures for trust in e-banking?
What is the relationship between perception of security and trust?
Phase 1: Identify measure
Feedback
Pilot Study
Phase 2 & 3: Survey and Analysis
Questionnaire: Section 1
Questionnaire: Section 2
The presence of security mechanisms positively affects a user's perception of security.
H2: The presence of security mechanisms negatively affects a user's perception of security.

**Figure 3.3 :Data Mapping**

## 3.6 Limitations of Research

The research aims at identifying the relationship between security and trust in e-banking and measuring the impact of the former on the latter. The time and budget constraints for the dissertation resulted in some limitations in the research process. First, the data collected through the questionnaire to validate the hypotheses developed is quantitative in nature. Due to time restrictions, collection of qualitative data through methods such as interviews could not be carried out. The use of quantitative and qualitative data would add to the validity and reliability of the study (Collis & Hussey, 2003).

Another limitation in this research is the sample chose, which consist of university students. While the random sampling approach ensured diversity in the sample, it is limited only to students. Obtaining data from a larger subset of the population provided additional validity to the data collected and the results obtained.

These are some of the limitations of the chosen research methodology.

## 3.7 Conclusion

The research model developed in this study captures the nature of the relationship between security and trust in electronic banking. There are two main hypotheses that form the basis of the model. Firstly, it is hypothesised that security mechanisms have a positive impact on consumers' perception of security. The second hypothesis states that perception of security has a positive impact of consumer trust in e-banking. The impact of mechanisms is considered individually according to the various security objectives that were identified in Chapter 2.

To verify this model, a survey methodology was found to suitable. A preliminary step in this research is to identify measurement items for security and trust from prior literature and verify these through a pilot study. This was then followed by the collection of data via a questionnaire. A random sample of students was selected for the study. While this sample is a small subset of the e-banking customer population, the diversity on the campus ensures that this sample is representative of the population.

Statistical analysis methods were employed to test the data and validate the research model and hypotheses. The measurement items were tested and validated using Cronbach’s alpha and CFA and regression testing was to be carried out using SEM.

# Chapter 4

# Report on Field Findings

## 4.1 Introduction

The previous chapter outlines\d steps that the research had followed to test and validate the research model that was developed. In this chapter, the results obtained at different steps during the research are presented. The first phase, which included identification of the measurement items for security and trust, was based on the review of literature. Modification of these items and the presentation of the items were carried out based on the findings of a pilot study.

The analyses of the data collected using SEM follows a pre-defined set of steps which translates the research model into a measurement and structural model that are used to assess how well the data fits the hypothesised research model. The weighting of the causal paths represent the relationship between different constructs and are used to test hypothesis.

In this research, a variety of measures such as Cronbach's alpha, composite reliability, convergent validity and so on are used to ensure that the data is reliable and valid. Fit indices such as Chi-square statistics, GFI, AGFI and so on are analysed to test the model fit. Finally, once the model fit is established, the hypotheses developed in Chapter 3 are tested based on the path estimates obtained.

The results of the pilot study are presented in Section 4.2 followed by details on the survey response in Section 4.3. The field findings including the data reliability and validity tests along with the model analyses are presented in Section 4.4. Finally, the conclusion follows in 4.5.

## 4.2 Pilot study

The pilot study included a review of the questionnaire by a group of experts. The questionnaires were sent for reviewing to 12 experts and feedback was received from 9. 3 experts were unable to respond due as the time was inconvenient for them. The response received was deemed to be sufficient as the initial aim was to receive feedback from 8-12 experts.

The first major change introduced was the rewording of all the items on Perception of Non repudiation (See Appendix B, Q4a, b and c). All reviewers found these items difficult to understand. These items were reworded based on the feedback received to better convey the underlying meaning of the questions. Along with this, the sub-section headers under perception of security were also deleted as the meaning of terms such as Perception of Non-repudiation and Perception of Availability were found difficult to comprehend.

The third change introduced was the addition on a section on general questions. These questions were added primarily because they would provide valuable information on the participants of this study. The experts also felt that asking personal questions would make the participants feel more involved and increase willingness to participate.

Another suggestion to change the scale from being worded ‘strongly disagree’ to ‘strongly agree’ to a numerical scale from -2 to +2 was discarded as these majority of the reviewers found this to be harder to follow. Scaling of questionnaire was an important aspect, as wording the responses from ‘Strongly Agree’ to ‘Strongly Disagree’ could be somewhat ambiguous because of the neutral/undecided option. This answer option can be interpreted as the participant has no knowledge and hence is not sure about the answer, or may hold a neutral position. This could inturn affect the overall result. The use of Strongly Agree/Disagree is also lead the participants to be biased towards the positively or favourable worded items in the scale. To mitigate the effect of such biases in the scale, positively and negatively worded questions were included. No items were deleted as the questions were found relevant and the layout remained unchanged.

## 4.3 Survey Response

A total of 138 responses were collected from students at the AUT campus. The age group of majority of the participants, being students, was between 20 and 30 (almost 60%) and 40% included participants below and above this age. This sample also had almost equal number of male and female participants.

Random sampling was ensured by approaching every third person passed on the campus. The data was collected by approaching participants directly and the number of participants who declined was not counted as part of the sample. Thus, calculating the rate of response would not be applicable.

From the total responses collected, 133 responses did not have any missing data. Five participants did not complete the questionnaire and data was missing for analysis of one of more constructs. It was decided that data from these questionnaires would not be included for data analysis as the software used for analysis would exclude these while analysing the information.

The 133 responses collected were marginally above the 130 mark aimed for giving a power of 80% at significance level of 0.05. As an adequate response was received for the survey within the allocated one week of data collection additional time was not spent to collect more responses.

## 4.4 Field Findings

The model developed in Chapter 3 represents the relationships between different the constructs. This model was validated with SEM using software packages SPSS 15.0 and AMOS 7.0. Before the model was validated, the measurement items of the questionnaire were studied for reliability and validity. The information related to the data collected and the results of the analysis are discussed in this section.

The descriptive statistics of the participants are presented in section 4.4.1. The initial steps of the SEM technique which include building a theoretical, path, measurement and structural model are explained in Section 4.4.2. This is followed by the specification of the analysis techniques (Section 4.4.3.) and analysis of the measurement items (Section 4.4.4). Analyses of the fit indices are explained in Section 4.4.5 (Overall fit indices), Section 4.4.6 (Measurement Fit indices) and Section 4.4.7 (Structural fit indices)

### *4.4.1 Descriptive statistics*

As noted in Section 4.3, the number of male and female participants in this survey was almost equal and a majority of them were between the age group of 20-29. As the participants were students, it was expected that a majority of them would fall into this age group.

A large number of participants (≈ 85%) had experience with using the internet for more than year at the time the survey was conducted. From this sample the number of people with internet banking experience over a year was marginally greater than those with lesser experience.

A summary of the descriptive statistics of the participants is presented in Table 4.1.

**Table 4.1: Descriptive statistics**

| | | **Percentage** |
|---|---|---|
| **Gender** | Male | 51.13 % |
| | Female | 48.87 % |
| **Age Group** | <20 | 27.06 % |
| | 20-29 | 63.15 % |
| | 30-39 | 7.5 % |
| | 40-49 | 1.5 % |
| | >50 | 0.75 % |
| **No. of years of Internet experience** | <1 | 15.78 % |
| | >1 | 84.21 % |
| **No. of years of internet banking experience** | <1 | 38.34 % |
| | >1 | 61.65 % |

### *4.4.2 Analysis of Research model*

Analysing the research model that was developed in Chapter 3 would make use of the Structured Equation Modelling technique. SEM uses a measurement and a structural model to analyse the data and validate the relationships between constructs (Anderson et al., 1998). The measurement model establishes a link between the latent variables and their indicators and the structural model studies the relationships between the constructs (Dhillon et al., 2007).

According to Anderson et al. (1998), the first step in SEM is to develop a theoretical model that represents the relationships between the constructs as indicated by previous studies. Schumaker & Lomax (2004), state that all available theory, research and information should be used to determine the variables that are included and the relationships between them. The theoretical model is developed prior to data analysis and the research model presented in Chapter 3 (Figure 3.2) represents the theoretical model for this study.

Further, the measurement and structural models are developed based on the theoretical model. The measurement model represents the confirmatory factor model that is used to test if the latent variables are measured well using the by using the available observed variable data and the structural model represents the relationship between these variable (Schumaker & Lomax, 2004). A path model that shows the causal relationships between the variables is used to represent this information.

A conceptual model that represents the path model and includes information on the measurement and structural models of SEM is defined as described by Merisavo et al. (2007). This model shows the causal pathways between the constructs and the relationship between the observed and latent variables (See Figure 4.1). While this model captures the measurement and structural model, these models are analysed independently used separate fit indices. Thus, a two-step SEM modelling approach is used (Anderson et al., 1998).

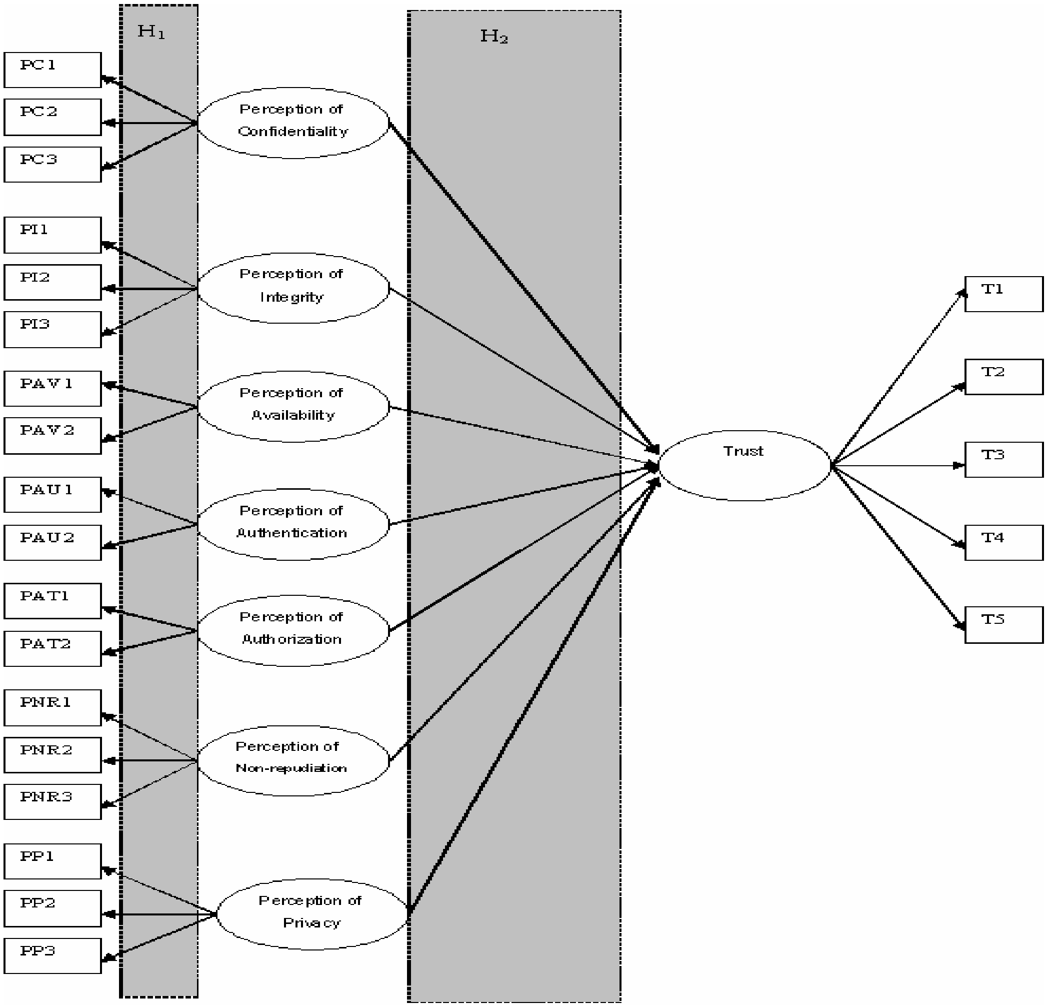
H1
H2
PC1
PC2
PC3
PI1
PI2
PI3
PAV1
PAV2
PAU1
PAU2
PAT1
PAT2
PNR1
PNR2
PNR3
PP1
PP2
PP3
Perception of Confidentiality
Perception of Integrity
Perception of Availability
Perception of Authentication
Perception of Authorization
Perception of Non-repudiation
Perception of Privacy
Trust
T1
T2
T3
T4
T5

**Figure 4.1: Path model**

### *4.4.3 Specification of the Analysis techniques*

SEM involves a number of analyses properties and techniques that must be identified before the model is tested. It was ensured that each construct has multiple indicators as a single indicator would require an estimation of the reliability before analyses (Anderson et al., 1998). Instead, the reliabilities of each construct would be empirically estimated to test the measurement model fit (See Section 4.4.4).

The correlation matrix (See Appendix C) was chosen as the matrix for inputting data as opposed to the variance-covariance matrix. The correlation matrix as it allows us to directly compare the coefficients in a model (Anderson et al., 1998) and is also useful when a single sample is tested (Suh & Han, 2003). The correlation matrix is also considered to be a standardised variance –covariance matrix (Anderson et al., 1998).

Maximum Likelihood estimation was used for estimation of the parameters and standard errors for each parameter. This procedure was chosen as it appropriate for a sample size between 100 and 150 (Anderson et al., 1998) and does not become extremely sensitive to data changes for this sample size. Also, direct estimation was chosen as the estimation technique as it is appropriate for calculating model estimates for a single sample (Anderson et al., 1998).

### *4.4.4 Analysis of Measurement items*

Reliability and validity of the items was tested using several measurements. The reliability of the measurement items was tested using Cronbach's alpha. Cronbach's alpha is dependent on the correlation between the items, and a higher degree of correlations is represented by a higher value of alpha. Thus, this provides an indication of the internal reliability of the measurement items under consideration.

The suggested alpha value should be greater than 0.7 for the items to be considered reliable (Suh & Han, 2003; Merisavo et al., 2007). Items with lower alpha values display low internal reliability and should not be considered for while analysing testing the model. In this study, Perception of Availability and Authorization displayed the highest internal reliability (alpha = 0.81) and Perception of Privacy and Trust had the lowest alpha value of 0.7 (See Table 4.2). As all the constructs had alpha values greater than the acceptable alpha value all items were retained in the study.

**Table 4.2: Reliability of Measurement items**

| Construct | Cronbach's alpha (>0.7) |
|---|---|
| Perceived Confidentiality | 0.71 |
| Perceived Integrity | 0.76 |
| Perceived Availability | 0.81 |
| Perceived Authentication | 0.71 |
| Perceived Authorization | 0.81 |
| Perceived Non -repudiation | 0.71 |
| Perceived Privacy | 0.70 |
| Trust | 0.70 |

The validity of the measurement items was analysed using construct validity test. Construct validity tests if the items are measuring the construct they are meant to measure. This include analysis of convergent and discriminant validity. Convergent validity examines if the measurement items all correspond with the construct. This validity was tested by examining the factor loadings of each item and the fit indices of the model. Estimating the factor loadings with the Maximum Likelihood Estimation procedure resulted in a small residual error variance on item PAT1 (Refer to table 4.3). To remove the identification problem a single additional constraint was added. As the negative residual value obtained was almost negligible (-0.05), Anderson et al. (1998) recommend that the variance be fixed to a small positive value to enable the researcher to continue with the calculation of the model estimates. Thus, this variance was set to small positive value of 0.05 and it would not greatly affect the estimated values obtained for the causal paths because this value is also negligible.

The recommended level of factor loadings, as noted by Suh & Han (2003), should be above the value of 0.6. All items except PC1, PNR3, T4 and T5 (Refer to table 4.3) are above this level. Suh & Han (2003) also noted that items that surpass the lower limit of 0.3 can still be used for analysis of the model fit. Hence, these items were retained for analysis. Along with these measurements, the fit indices of the model also suggested the data fit the model (See Section 4.4.5 for discussion of fit indices). Thus, convergent validity was verified for the items. Table 4.3 summarizes the factor loadings of each item.

**Table 4.3: Factor loadings of measurement items**

| Construct | Item | Factor loading |
|---|---|---|
| Confidentiality | PC1 | 0.442 |
| | PC2 | 0.740 |
| | PC3 | 0.821 |
| Integrity | PI1 | 0.731 |
| | PI2 | 0.688 |
| | PI3 | 0.725 |
| Availability | PAV1 | 0.807 |
| | PAV2 | 0.845 |
| Authentication | PAU1 | 0.818 |
| | PAU2 | 0.678 |
| Authorization | PAT1 | 0.982 |
| | PAT2 | 0.687 |

| | | |
|---|---|---|
| Non-repudiation | PNR1 | 0.672 |
| | PNR2 | 0.754 |
| | PNR3 | 0.596 |
| Privacy | PP1 | 0.771 |
| | PP2 | 0.729 |
| | PP3 | 0.772 |
| Trust | T1 | 0.790 |
| | T2 | 0.663 |
| | T3 | 0.612 |
| | T4 | 0.508 |
| | T5 | 0.361 |

Discriminant validity ensures that the individual constructs are indeed distinct and that no similarities exist between them. This validity was tested using the Chi-square difference test between the seven constructs of perception of security (See Table 4.4). The highest difference in the chi-square values ($\chi^2$ difference) is between Perception of Confidentiality and Authorization with a value of 117. 5. The lowest difference of 24.3 is between Perception of Availability and Privacy. According to Schumaker & Lomax (2004), the recommended value of chi-square for the obtained degrees of freedom between the constructs should be above 3.84. All the chi-square difference values surpassed the recommended threshold showing that each construct was indeed distinct. As both convergent and discriminant validity of the data is confirmed, the items passed construct validity tests.

**Table 4.4: Chi-square difference results**

| | **Model with Fixed Correlation** | | **Model with Free Correlation** | | $\chi^2$ **Difference** |
|---|---|---|---|---|---|
| | **df** | $\chi^2$ | **df** | $\chi^2$ | |
| Confidentiality - Integrity | 42 | 131.2 | 41 | 50.7 | 80.5 |
| Confidentiality - Availability | 33 | 111.9 | 32 | 45.2 | 66.7 |
| Confidentiality - Authentication | 33 | 117.6 | 32 | 46.3 | 71.3 |
| Confidentiality - Authorization | 33 | 162.4 | 32 | 44.9 | 117.5 |
| Confidentiality - Non repudiation | 42 | 171.3 | 41 | 68.1 | 103.2 |
| Confidentiality - Privacy | 42 | 124.7 | 41 | 54.1 | 70.6 |
| Integrity - Availability | 33 | 102.5 | 32 | 50.1 | 52.4 |
| Integrity - Authentication | 33 | 108.8 | 32 | 42.8 | 66 |
| Integrity - Authorization | 33 | 82.9 | 32 | 39.3 | 43.6 |
| Integrity - Non repudiation | 42 | 144.2 | 41 | 52.3 | 91.9 |

| | | | | | |
|---|---|---|---|---|---|
| Integrity - Privacy | 42 | 101.2 | 41 | 49.6 | 51.6 |
| Availability - Authentication | 25 | 76.6 | 24 | 45.1 | 31.5 |
| Availability - Authorization | 25 | 86.6 | 24 | 41.2 | 45.4 |
| Availability - Non repudiation | 33 | 111.7 | 32 | 55.7 | 56 |
| Availability - Privacy | 33 | 74.9 | 32 | 50.6 | 24.3 |
| Authentication - Authorization | 25 | 78.1 | 24 | 34.8 | 43.3 |
| Authentication - Non repudiation | 33 | 107.3 | 32 | 51.8 | 55.5 |
| Authentication - Privacy | 33 | 78.8 | 32 | 51.1 | 27.7 |
| Authorization - Non repudiation | 33 | 94.1 | 32 | 49 | 45.1 |
| Authorization - Privacy | 33 | 118.2 | 32 | 45.6 | 72.6 |
| Non repudiation - Privacy | 42 | 144.4 | 41 | 65 | 79.4 |

### *4.4.5 Assessing Overall Model Fit*

A number of fit indices are generated to test how well the data fits the model defined. There are varying opinions on the fit indices that are most appropriate to be taken into consideration while studying the overall model fit, most researchers rely on the indices such as Chi-square statistics, GFI, AGFI, TFI (or NNFI) and so on. Each index is calculated and used to examine a certain aspect of the model, but when considered together they provide an overall view of how well the data fits the given model. Table 4.5 summarises the values of some of the commonly examined indices.

**Table 4.5: Model Fit Indices**

| Index | Value | Recommended Value |
|---|---|---|
| Chi-square($\chi^2$) | 242.469 | |
| P-value | 0.014 | |
| Degrees of Freedom (df) | 209 | |
| $\chi^2$/df | 1.228 | <5.0 |
| Goodness of Fit (GFI) | 0.860 | >0.8 |
| Adjusted Goodness of Fit (AGFI) | 0.816 | >0.8 |
| Root-mean-square error of approximation (RMSEA) | 0.042 | <0.05 |
| Tucker-Lewis index (TFI) | 0.923 | >0.9 |
| Comparative Fit Index (CFI) | 0.936 | >0.9 |

Amos 7.0, along with the proposed model, also provides the indices for a saturated and an independence model. In the independence model the variables are assumed to be uncorrelated with the dependents, i.e., there are no paths in the models and the

saturated model has no constraints and all paths are included in this model (Schumaker & Lomax, 2004). Thus, the first check while evaluating the model is to ensure the chi-square value does not exceed the chi-square value of the independence model. The value should be in between the chi-square values of the saturated and independence models. The obtained value lies between the chi-square value for the saturated model ($\chi^2 = 0$) and the independence model ($\chi^2 = 1002.933$).

The recommended chi-square should be close to zero to indicate that proposed model matches the actual mode. A significant Chi-square value is obtained ($\chi^2 = 242.469$) showing that the actual model differs from the proposed model. But, the Chi-square statistics are sensitive to sample sizes and not always accurate in determining the model fit (Schumaker & Lomax, 2004). Instead, the ratio of Chi-square to the degrees of freedom ($\chi^2$/df) is considered a better measure and it is recommended to be below 5.0 (Suh & Han, 2003). The value of $\chi^2$/df is obtained as 1.228 and hence shows the proposed model is close to the actual model.

The Goodness of Fit Index (GFI) is considered acceptable above 0.9 by some researchers (Schumaker & Lomax, 2004) but a value above 0.8 is considered to an acceptable indication of a good fit (Suh & Han, 2003). Similarly, the Adjusted Goodness of Fit Index (AGFI) is above the suggested value of 0.8. Other indices such as TFI and CFI surpass the recommended level of 0.9 and RMSEA is below the 0.05 value mark. All these indices are suggestive of a good model and indicate that the data fits the given model well. Thus, overall model fit is evaluated.

### *4.4.6 Assessing Measurement model fit*

The measurement model fit evaluates the measurement of each construct (Anderson et al., 1998) and is considered to be a more rigorous test for assessing the items being used. The method of evaluating the measurement model fit is primarily tested the composite reliability and variances extracted for each construct (Anderson et al., 1998). Composite reliability tests the reliability of each construct based on the item loadings and the variance captures the amount of variance in the construct based on the measurement errors.

Confirmatory factor analysis was also used to evaluate the composite reliability of the items. The standardized factor loadings and the measurement error of each item was used to calculate this measure based on the formula defined by (Anderson et al., 1998). According to Anderson et al. (1998), the composite reliability should exceed 0.7 and all the constructs are above this threshold value. The average variance extracted should be above 0.5, which is demonstrated by all the constructs showing that the indicators represent their respective variables.

The summary of the composite reliability and variance extracted are presented in Table 4.6.

**Table 4.6: Composite Reliability and Variance Extracted**

| Construct | Composite Reliability (>0.7) | Average Variance Extracted (>0.5) |
|---|---|---|
| Perceived Confidentiality | 0.72 | 0.50 |
| Perceived Integrity | 0.76 | 0.52 |
| Perceived Availability | 0.81 | 0.69 |
| Perceived Authentication | 0.71 | 0.56 |
| Perceived Authorization | 0.83 | 0.72 |
| Perceived Non -repudiation | 0.71 | 0.51 |
| Perceived Privacy | 0.80 | 0.58 |
| Trust | 0.70 | 0.50 |

### *4.4.7 Assessing Structural model fit*

The structural model fit is examined by studying the estimated coefficients of the causal pathways along with the critical ratio (t-value) for the estimates. A model is found to be structurally fit if path estimates that are obtained support the underlying hypotheses of the model. Therefore, the hypotheses developed in Chapter 3 will also be tested while assessing the structural model.

For analyses of the structural model, the significance level ($\propto$ - value) was specified to be 0.05. The estimates and t-values for the causal paths between perception of security and trust at this significance level are shown in Figure 4.2. The t-values appear in brackets in the diagram. The critical ratio for the path between perception of privacy and trust is significant at the significance level of 0.05 as it is above 1.96 (Anderson et al., 1998).

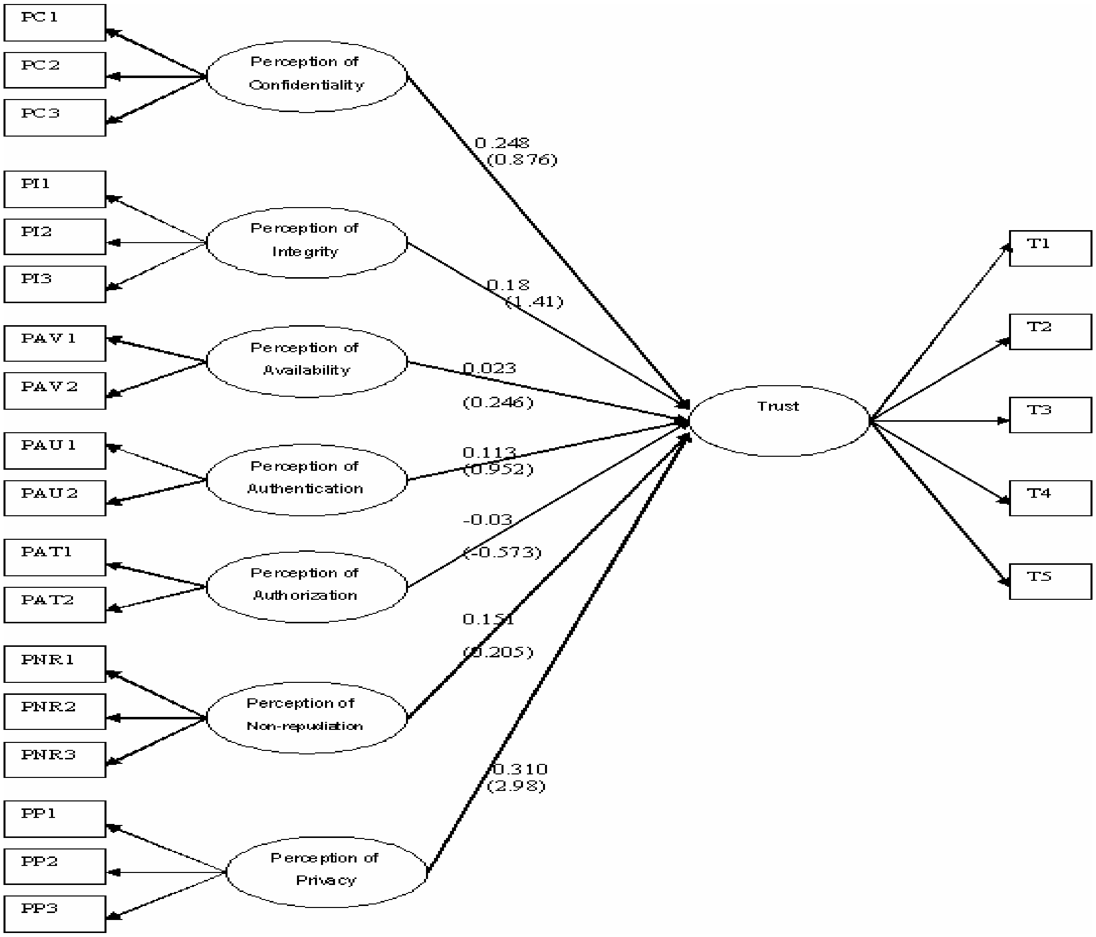

**Figure 4.2: Estimates and Critical Ratios**

Each indicator of the construct of perception of security show the relationship between different security mechanisms and their perception constructs. The mean estimates for the loads of indicators on their respective constructs are shown in Table 4.7.

**Table 4.7: Mean estimates of indicators**

| Construct | Mean estimates of indicators |
|---|---|
| Perception of Confidentiality | 0.667 |
| Perception of Integrity | 0.714 |
| Perception of Availability | 0.826 |
| Perception of Authentication | 0.748 |
| Perception of Authorization | 0.834 |
| Perception of Non repudiation | 0.674 |
| Perception of Privacy | 0.757 |

The first hypothesis, $H_1$ states that the presence of security mechanisms has a positive impact on the perception of security. Further, the hypothesis is decomposed to consider each security component separately, for example, the presence of confidentiality mechanisms has a positive impact on perception of security. From the values in Table 4.7 it can be noted that the indicators perception of security have a significant weighting on the components of perceived security that they are associated with. These indicators represent the perception of the security based on the security mechanisms that affect it. Mechanisms that indicate the presence of availability and authorization show the highest weighting on the individual component of perception of security. From these values, it can be concluded that the mechanisms of security such as confidentiality, integrity and so on have significant impact on the perception of security. This, Hypothesis $H_1$, which includes $H_{1a}$ to $H_{1g}$ can be accepted as the estimates show that the presence of security mechanisms have a positive impact on perception of security.

The second hypothesis, $H_2$ considers the overall impact of perception of security on trust. Each individual construct representing perception of security is examined. The impact of perception privacy and confidentiality are found to be highest on trust (0.310 and 0.248 respectively). Perceptions of integrity, authentication and non-repudiation also have a positive impact on trust, but lower than that of perceived privacy and confidentiality. Availability has a minimal positive impact while authorization shows a small negative impact on trust. As each construct is a component of perceived security, their combined effect on trust represents the impact of perception of security on trust. Thus, combining the estimates of the individual components to get the weighting of perception of security on trust, it can be noted that perception of security has a positive impact on trust but the impact is not significant. Therefore, $H_2$ is not supported.

Along with the path estimates and t-values, the value of coefficient of determination ($R^2$) is also examined as part of the structural model fit assessment. This value for trust is 13.2%. This shows the perception of security accounts for 13.2% variance in trust. While this value is lower than recommended, the value of $R^2$ is dependent on the sample size, significance level and number of independent variables with sample size having the maximum impact (Anderson et al., 1998). Smaller sample sizes such as N=133 would show a relatively low value of $R^2$.

## 4.5 Conclusion

The first phase in this research, which included the modification of measurement items and the survey questionnaires through a pilot study, resulted in a few changes in the items. Rewording of non-repudiation items and including a section on general questions were some of the most significant changes introduced.

The survey was conducted using sample size of 133 (excluding 5 with missing data), to obtain a power function of 80% at a significance level of 0.05. This was marginally exceeded the expected size of 130 participants. There were almost equal numbers of male and female participants with a majority of the participants having internet banking experience over a year.

The reliability measures, using Cronbach's alpha, showed that all the items used for each construct passed the accepted value of 0.7. Similarly, validity testing of the items, using convergent validity showed that most items were above the expected 0.6 value while the all items were above the acceptable 0.3 threshold; hence all items were retained in the analysis. Discriminant validity testing using Chi-square difference tests showed that each construct of perceived security was indeed distinct.
The overall fit indices indicate a good model fit. The chi- square value was significant showing that the proposed model an actual model differs, but as it is dependent on sample size, the ratio of chi-square to degrees of freedom was considered. The GFI and AGFI indices were above the accepted value of 0.8 while TFI and CFI above 0.9 and RMSEA below the 0.05 threshold.

Composite validity and average variance tests, used to test the measurement model fit index showed were both above the 0.7 and 0.5 thresholds that indicate a good level of fit.

The path estimates that were obtained for the structural model validated both hypothesis, $H_1$ and $H_{2.}$ The mechanisms indicating authentication, authorization, privacy and availability showed the highest weighting on the respective components of perceived security. Perception of security had a positive impact on trust, but the results indicated that this impact was not significant. Perception of confidentiality and Privacy had the most significant impact on consumer trust.

# Chapter 5

# Discussion and Recommendations

## 5.1 Introduction

The primary research question for this study is to find out the impact of security on consumer trust in online banking. As it was pointed out it Chapter 2, security for a user is represented as a perception, and this perception is built based on the presence or absence of security mechanisms. Thus, to answer the main research questions, two sub-questions were formulated, to study the impact of security mechanisms on perception of security and the impact of perception of security on trust

In the previous chapter, Chapter 4, the findings of a survey undertaken were presented. The results of analysing the data using Structured Equation Modelling showed that security mechanisms had a positive impact on perception of security. Perception of security had a positive, but negligible impact on trust. In this Chapter, the comparison of the findings of this research would be compared and contrasted with findings from similar research.

In the following section (Section 5.2) the discussion of the findings are presented. This includes assessing the link of the findings to the main theoretical questions and comparing similar studies. Section 5.3 then discusses the limitations of this study which leads into the discussion of further research opportunities in Section 5.4. Finally, the conclusion is presented in Section 5.5

## 5.2 Discussion of Findings

The results obtained from the analysis discussed in Chapter 4 confirm the existence of a relationship between security and trust and further provide an understanding of the nature of the relationship between the two concepts. As the aim of this research is largely decomposed into assessing the impact of security mechanisms on perception of security and studying the impact of perception of security on trust, the findings related to the two hypotheses developed are discussed separately in Section 5.2.1 and Section 5.2.2 respectively.

### *5.2.1 Security Mechanisms and Perception of Security*

In Chapter 2 it was noted that security mechanisms are the antecedents to perceived security and they could encourage or discourage a user from interacting with online banking systems (Ally & Toleman, 2005, Suh & Han, 2003). These security mechanisms would have the potential to affect a user's perception if they are visible and indicated through the user interface (Johnston et al., 2003). Based on this knowledge, the first hypothesis developed in this study stated that the presence of security mechanisms would positively affect a user's perception of security in online banking.

The results from the analysis of the data collected in this research suggest that the presence of security mechanisms in an online banking interface have a positive impact on a perceived security. As seen in Chapter 2, previous research had confirmed that security mechanisms play a role in development of a user's perception of security. The results show that these mechanisms have a very significant positive impact on perception. These results are in agreement with the findings from previous literature including Turner et al. (2001), Ally & Toleman (2005). These studies were the basis for hypotheses one as indicated in Chapters 2 and 3.

The findings of this research have significant implications for online banking security. They show that the participants were highly aware of these security indicators and their view of the websites security is highly dependent on these indicators. Thus, this indicates the importance of educating users about security mechanisms being used by the online system. Turner et al. (2001) suggested that conveying features through the interface is one of the criteria for building the security image of the interface. The importance of visible indicators for security had also been highlighted by Johnston et al. (2003) and Ally and Toleman (2005), and the findings from this study confirm and further suggest that visible indicators are one of the most important antecedents of perceived security.

Security is viewed as a composite construct composed of several objectives. The role of security mechanisms in building the perception of each of these objectives can also be individually evaluated. Mechanisms that indicate availability, authentication, authorization and privacy had the highest impact on the perception of their respective security objectives. From the steps of e-banking activities outlined by Classens et al. (2002), the objectives that define security at each point during a user's interaction with the system are defined. It is seen that the different security mechanisms that contribute to perception of authentication, authorization, availability and privacy together cover all the step of e-banking activities. This indicates the user is aware of and is affected by different mechanisms throughout his interaction with the system. Thus, indicators of different facets of security should be present and the user should be informed about them through the interface at every point during his e-banking activities.

The main question in this research addresses the impact of security on trust in e-banking as previous research identified security awareness as a factor that builds trust. Studying the results in this research, visible indicators of security mechanisms are found to play a vital role in improving the awareness of security in the online banking environment. Thus, banking websites should incorporate and ensure that their security measures are visible to the users.

### *5.2.2 Perceived Security and Trust*

The perception of security was identified as one of the most important factors that assist in building trust in an online environment by researchers such as Bargh et al. (2002), Lim (2003) and so on. The ambiguous nature of trust arises from the many dimensions that it comprises of, including institution based trust, disposition to trust, and so on. Studying these dimensions it was noted that institution based trust was the component of trust that would be affected by external environmental factors which include security. Belanger et al. (2002) suggested that security would be the first factor that should be considered in building institution based trust and hence overall trust. Thus, it was hypothesised that the perception of security in online banking would have a positive impact on trust.

The findings from this research showed that the overall perception of security had a marginal positive impact on a user's trust in online banking. Lim (2003) had identified two relationships that link perceived security and trust. The research model that was built in this study chose to study the impact on perceived security on trust, and the relationship chosen from Lim (2003), states that there is a positive impact. The results from the study show that this relationship is indeed true and that perception of security can contribute to the development of trust in online banking applications.

While, the result did indicate a positive impact, the significance of this impact was negligible. These findings align with results from studies such as Suh and Han (2003), Yousafzai et al. (2005) to show that perceived security does have a positive impact on user trust, but the level of this impact varies from other research reports. This variation could have arisen due to differences in the meaning of perception of security from these studies. Chellapa (2002) shows that perception of security has a high level of impact on trust, but in this study a user's perception is evaluated as a whole and the components contribute to this perception are not considered. Unlike this and similar research studies, in this study perception of security is considered to be built based on security mechanisms of the websites.

In Section 5.2.1, it was noted that security mechanisms play a vital role in developing a user's perception of security, but other factors including brand name, prior knowledge on security and so on also contribute in the development of this perception (Turner et al. 2001). Thus, the impact that is evaluated in this study is that of perceived security, built from security mechanisms, on trust. Belanger et al. (2002) also found that the level of trust in a user could be high in spite of indices for security in a website being low. Their results indicate that perceived security built on these security indices would not have a significant impact on trust. Therefore, this could have contributed to the variation in the level of impact from results noted in similar studies.

Evaluating the impact of individual components of security on trust it was noted that perception of confidentiality and privacy had the most significant impact on trust. The impact of perceived privacy on trust was found to be the highest and this is similar to the results obtained by Chellapa (2002). The impact of other components of perceived security on trust was not found to be significant at the significance level of 0.05. Thus, perceptions built on mechanisms for availability, integrity and so on do not considerably affect consumer trust.

The link between security and trust in e-banking as identified in this research shows that security has a positive impact on trust. Perceived security which is built based on security indicators shows that the impact on trust is not very significant. Perceived privacy is the component of security that has a significant impact on consumer trust in online banking. These results reflect the nature of the relationship between the two constructs, security and trust, in online banking.

## 5.3 Limitations of Research

Several constraints in terms of time and budget introduced several limitations in this research. Time restrictions defined the scope of the dissertation and the environment chosen for studying the link between security and trust was limited to the e-banking environment. Along with this several limitations related to the theoretical model are noted.

In Section 5.2.2 we noted that the definition of perceived security for this study is the perception built on the visible security mechanisms in the interface. It was also noted that security mechanisms play an important role in the development of this perception but certain other factors have also been shown to play a role in this development. This was one of the main limitations in the theoretical model, that it did not include and study the role of these factors.

The restricted time frame also introduced certain limitations in the research methodology. These limitations were discussed in detail in Chapter 3 while reviewing the research design. Analysis of the data further revealed that the sample which was restricted to students on a campus, had majority of the participants upto the age of 30 years. Representatives of higher age groups were only a small percentage in this study. While not all age groups were represented equally, random sampling did ensure diversity in the sample in terms of gender and internet banking experience.

Another limitation in the methodology was the use of only quantitative data to validate the research model. Using qualitative data would increase the reliability and the validity of the research findings. The data collected in this study did pass the reliability and validity tests but collecting qualitative data along with quantitative data would provide rich and informative details on the role of security and trust in e-banking.

The analysis in this research studies the security and trust in Internet banking by considering all participants as a single sample. But descriptive statistics of the participants would also help analysing these relationships for different groups of users based on prior banking experience, age group and so on. Limited time for analysis prevented the research from expanding the analysis to study how different demographics of people perceive security and its impact on trust.

These were some of the major limitations of this study and these limitations were mainly introduced due to time and budget restrictions.

## 5.4 Further Research

The limitations of this research outline various opportunities for further research work in understanding the relationship of security and trust in e-banking and other e-commerce applications in general. Due to time and budget constraints the scope of this dissertation was restricted, but using the findings of this study, a deeper understanding of the relationship between security and trust can be established.

This research concentrates on the effect of visible security mechanisms on perception of security. While security indicators are established to play a significant role in developing a user's perception of security, concentrating only on perception based on these restricts the scope of perceived security that is studied in relation to trust. Extending the definition of perceived security by including other factors that affect it such as brand name age, gender, culture and other characteristics of the users and interface would provide a broader outlook on perceived security (Chellappa, 2002). Their role in defining perception of security and consequently their effect on trust can be studied.

Turner et al. (2001) argued that prior knowledge on security mechanisms was an important factor that would decide the extent to which these mechanisms would affect a user's perception. Extending the research model developed in this paper to study the role of prior knowledge in defining the perceived security through indicators and their impact on trust would provide valuable information on how users interact with security and its impact on their level of trust in a banking website.

Trust has been identified as a multidimensional construct and developing consumer trust would require building each of the dimensions of trust. Trust development studies have found several other factors such as website design, brand name and marketing strategies (Patton, 2004) that are also linked to the improving levels of consumer trust. The current research model could be modified to study the relationship of other factors with trust. This would allow a comparison to be drawn between the level of impact of other factors and the impact of security. This knowledge would give a wider view of the role of security in trust development as compared to the other factors.

Further, researchers have identified the importance of security in developing willingness and acceptance of services based on its relationship with trust (Chellappa, 2002; Suh & Han, 2003). In Chapter 2, we also noted various other relationships between security and trust that included factors such as trusting behaviour and willingness. Building on the current hypothesised model, the relationship between perceived security, trust and other factors can be established. The role of perceived security and/ or trust in development of other intentions and behaviours in a user and the level of impact they have on the user can be identified.

Other research opportunities include the modification of the framework to suit other areas of e-commerce applications. As security and trust play a critical role in other e-commerce domains, the hypotheses can be extended to be tested in these domains. This would provide a generalized view of security mechanisms, perception and trust in e-commerce.

## 5.5 Conclusion

The discussion of the findings studied the significance of the results of this research for literature and practitioners dealing with security and trust in the e-banking environment. The presence of security mechanisms was found to have a significant positive impact on consumer trust. This implies that the users were highly aware of the indicators of these mechanisms. Thus, visible security mechanisms play an important role in the development of perception of security. The indicators of availability, authentication, authorization and privacy are found to have the maximum impact on perception.

The role of perceived security on trust as indicated by this study differed from results in other researches such as Suh & Han (2003), Yousafzai et al. (2005). This difference was attributed to the different definitions of perceived security in this research as compared to the other literature studied. Only the component of perceived security that develops based on security mechanisms is considered in this study. The results indicate that perceived security, based on visible security, has a negligible positive impact on trust. Perception of privacy had the highest and most significant impact on trust.

The limitations in this study were mainly introduced due to time and budget restrictions. The theoretical model considered on a limited definition of perception of security and thus results differed from other studies. The time restrictions were taken into consideration while developing the research design and introduced some limitations in the research methodology. The sample had participants that were students and hence majority of these participants were under the age of 30 years. Also, the questionnaire concentrated on collecting qualitative information and quantitative data was not considered.

Further research opportunities include studying the role of other factors such as age, knowledge and so on in defining perception of security and its impact on trust in e-banking. The role of security as compared to other trust building attributes in internet banking can also be evaluated. The research model can be extended to other e-commerce applications to study the role of security in developing trust. The model can also be extended to include factors such as willingness and trusting behaviours and study the interrelationship between these components,

Thus, the discussion highlights the importance of security mechanisms in the development of perceived security and also indicates that perception built on these indicators does not have a significant role in developing consumer trust in internet banking.

# Chapter 6

# Conclusion

## 6.1 Conclusions of the Research

The aim of this study was to study the level of impact of perceived security on trust in online banking. Security and trust have been identified as important aspects that need to be considered in e-commerce applications. To study the relationship between trust and security, the online banking environment was chosen. Electronic banking provided a suitable environment for this research as the banking activities involve exchange of sensitive personal information about users. This makes perception of security and consumer trust important factors for e-banking. As users interact with different security mechanisms at every stage during their interaction with the banking system, their effect on the users' perception of security and trust could be studied.

Using a survey, qualitative data was collected from a random sample of students on the AUT campus. The mixture of qualitative and quantitative data was not used due to time restrictions on the study. The use of random sampling ensured that a diverse range of internet users were included in this study. The data showed that there were equal number of male and female participants and majority of the participants had internet banking experience of over a year. But as the sample was based in a university and included students, majority of the participants were below the age group of thirty years. Hence, the results would be mostly applicable to internet users within this age group.

This data passed the tests for validity that included construct and determinant validity tests. Reliability of data was ensured by using measures such as Cronbach's alpha and composite reliability tests. Structured equation modelling that included confirmatory factor analysis showed that the data collected fit the proposed research model and hence the relationships between security mechanisms, perceived security and trust could be analysed.

Reviewing previous literature it was noted that different website factors were found to play an important role in the development of a user's perception of security. In developing this perception of security, indicators of security mechanisms were found to play an important role. Thus, it was hypothesised that the presence of security mechanisms had a positive impact on perceived security. The results supported this hypothesis and showed that the mechanisms that were indicated by the website had a significant impact on the participants' perceptions. Visible security mechanisms for privacy, availability, authentication and authorization had the maximum impact on the consumers' perceptions.

The strong correlation between visible security mechanisms and perception of security indicated that the users of internet banking websites are aware and influenced by the presence of these indicators. This further highlights the importance of indicating the types of mechanisms used and educating the users about these mechanisms. Users at every step note these indicators during their interaction with the banking system. Banking sites should maximise the use of security indicators in their interface to help establish a high perception of security in their consumers. The importance of visible security mechanisms in developing the perception of security was reinforced through these results.

The relationship between perceived security and trust as outlined by prior studies manifests itself in several different forms. To understand the impact of perception of security on trust one of these relationships was considered as the basis and it was hypothesised that perceived security would have a positive impact on trust. Perceived security had been identified as an important factor for building consumer confidence and trust across e-commerce applications. The results from the analysis showed that perceived security had a positive but negligible impact on trust. Therefore, the second hypothesis could not be accepted.

The results obtained for the second hypothesis varied from the results obtained in prior studies. The variation could be attributed to the differing view of perceived security from the other studies. The perception of security studied comprised only the component that is affected by security mechanisms. Security mechanism indicators were found to have an important role in developing the user's perception but studies have also found other website and consumer attributes to contribute to perception. The definition of perceived security differed from other studies and hence it could be concluded that this component of perception had a negligible impact on trust. Belanger et al. (2002) argued that the assurance of security leads to development of trust but also found that the indicators of security did not greatly affect trust. The results that were obtained in this research further showed that the perception of security built from these indices do not have a significant impact on a consumer's level of trust in e-banking.

The perception of privacy was the component of perceived security that had a significant positive impact on trust, while the other components did not greatly affect it. This implied that users concerns related to privacy of information are the highest and need assurance on all issues related to privacy of information. Online banking interfaces should inform their consumers on the methods used by them to ensure the privacy of the user's information and transactions. Thus, maximising effort to improve the perception of privacy would help increase the level of trust in e-banking applications.

The major findings of this research show the importance of security mechanisms in building users perception of security and that this perception does not have a significant impact on consumer trust in e-banking. The importance of perception of privacy for trust development is also highlighted in this study. The study provides mitigating evidence of a deeper understanding into the nature of the relationship between security and trust in online banking.

# References

Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information management, 21, 213-225.

Ally, M., & Toleman, M. (2005). A framework for assessing payment security mechanisms and security information on e-commerce web sites. Paper presented at the 9th Pacific Asia Conference on Information Systems (PACIS), Bangkok, Thailand.

Anderson, Tatham, & Black. (1998). Multivariate data Analysis (5th ed.): Prentice Hall.

Bargh, M., Janssen, W., & Smit, A. (2002). Trust and Security in E-business Transactions. Retrieved 21 October, 2006, from http://scholar.google.com/url?sa=U&q=https://doc.telin.nl/dscgi/ds.py/Get/File-22996/TIpaperWWW2002final_1.pdf

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems, 11, 245-270.

Chellappa, R. K. (2002). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Retrieved 4 March, 2007, from http://asura.usc.edu/~ram/rcf-papers/sec-priv.pdf

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management, 15(5/6), 358-368.

Claessens, J., Dem, V., Cock, D. D., Preneel, B., & Vandewalle, J. (2002). On the Security of Today's Online Electronic Banking Systems. Computers & Security, 21(3), 257-269.

Collis, J., & Hussey, R. (2003). Business Research (Second ed.): Palgrave Macmillan.

Dawis, R. V. (1987). Scale Construction. journal of Counceling Psychology, 34(4), 481-489.

Dhillon, G., Tejay, G., & Hong, W. (2007). Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations. Paper presented at the Proceedings of the 40th Hawaii International Conference on Systems Sciences, Hawaii.

Dillman, D. A. (2000). Mail and Internet Surveys (2nd ed.): John Wiley & Sons.

Egger, F. N. (2003). Evaluating the Customer Trust Experience in B2C ECommerce Environments.   Retrieved 28 September, 2006, from http://scholar.google.com/url?sa=U&q=http://computing.open.ac.uk/INTERACT 2003/Presentations/Egger.pdf

Gefen, D. (2000). E-commerce: the role of familiarity and trust. . Omega: The International Journal of Management Science, 28, 725-737.

Ghosh, A. K. (1998). E-commerce Security: Weak links, Best Defences: Wiley Computer.

Gollman, D. (2000). E-commerce Security. Computing and Control Engineering, 116-118.

Grabner-Krautera, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. International Journal on Human-Computer Studies, 58, 783-812.

Grandison, T., & Sloman, M. (2000). A Survey of Trust in Internet Applications. IEEE Communications surveys and tutorials, 3(4), 2-30.

Hawkins, S., Yen, D. C., & Chou, D. C. (2000). Awareness and challenges of Internet security. Information Management & Computer Security, 8(3), 131-143.

Herrmann, G., & Herrmann, P. (2004). Introduction: Security and Trust in Electronic Commerce. Electronic Commerce Research, 4, 5-7.

Hertzum, M., Juul, N. C., Jørgensen, N., & Nørgaard., M. (2004). Usable Security and E-Banking: Ease of Use vis-à-vis Security. Paper presented at the Proceedings of the OZCHI 2004 Conference, Australia.

Hutchinson, D., & Warren, M. (2003). Security for Internet banking: a framework. Logistics Information Management, 16(1), 64-73.

Jarvenpaa., S., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. Information Technology and Management, 1(1-2), 45-71.

Johnston, J., Eloff, J. H. P., & Labuschagne, L. (2003). Security and human computer interfaces. Computers & Security, 22(8), 675-684.

Jones, S., Wilikens, M., Morris, P., & Masera, M. (2000). Trust requirements in E-business, a conceptual framework for understanding the needs and concerns of different stakeholders. Communications of the ACM, 43(12).

Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. The Journal of Conflict Resolution, 14(3), 357-368.

Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. Information management & Computer Security, 10(4), 149-158.

Knorr, K., & Röhrig, S. (2000). Security of Electronic Business Applications: Structure and Quantification. Paper presented at the Proceedings of the First International Conference on Electronic Commerce and Web Technologies.

Lee, M. K. O., & Turban, E. (2001). A trust model for consumer Internet shopping. International Journal of Electronic Commerce Research, 6(1), 75-91.

Lee, P.-M. (2002). Behavioral Model of Online Purchasers in E-Commerce Environment. Electronic Commerce Research, 2, 75-85.

Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: an empirical study. Information and management, 39, 283-295.

Lim, N. (2003). C onsumers' perceived risk: sources versus consequences. Electronic Commerce Research and Applications, 2, 216-228.

M.K., C., & lee, M. K. O. (2001). Trust In internet shopping:Instrument Development and Validation through classical and modern approaches. Journal of Global Information management, 9(3), 23-35.

Maijala, V. (2004). Outlook of the Information Security in E-Business. Retrieved 8 October, 2006, from http://www.tml.tkk.fi/Publications/Thesis/maijala.pdf#search=%22security%20mechanisms%3Ee-business%3Ethesis%22

Mayer, R. C., Davis, j. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 10(3), 709-734.

McCullagh, A. (1998). E-commerce - A matter of TRUST. Retrieved 15 October, 2006, from http://www.acs.org.au/president/1998/past/io98/etrust.rtf

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-361.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. The Academy of Management Review;, 23(3), 473-490.

Merisavo, M., Kajalo, S., Karjaluoto, H., Virtanen, V., Salmenkivi, S., Raulas, M., et al. (2007). An Empirical Study of the Drivers of Consumer Acceptance of Mobile Advertising [Electronic Version]. Journal of Interactive Advertising from http://www.jiad.org/vol7/no2/merisavo/index.htm.

Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. International Journal of Bank MArketing, 21(1), 5-15.

Nilsson, M., Adams, A., & Herd, S. (2005). Building Security and Trust in Online Banking. Paper presented at the Conference on Human Factors in Computing Systems, Portland, USA.

Oppliger, R. (1999). Shaping the Research Agenda for Security in E-Commerce. Paper presented at the Proceedings of the 10th International Workshop on Database & Expert Systems Applications

Oscarson, P. (2003). Information Security Fundamentals, Graphical Conceptualisations for Understanding: Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden.

Otto, J. R., & Chung, Q. B. (2000). A Framework for Cyber-Enhanced Retailing: Integrating E-Commerce Retailing with Brick-and-Mortar Retailing. Electronic Markets, 10(13), 185-191.

Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age. Security Management Practices, 13-27.

Patton, M. A. (2004). Technologies for Trust in Electronic Commerce. Electronic Commerce Research,, 4, 9-21.

Ratnasingham, P., & Kumar, K. (2000). Trading partner trust in electronic commerce participation. Paper presented at the Proceedings of the twenty first international conferences on Information systems.

Schumaker, R., & Lomax, R. (2004). A Beginner's Guide to Structural Equation Modeling (Second ed.): Lawrence Erlbaum Associates.

Slyke, C. V., Belanger, F., & Comunale, C. L. (2004). Factors Influencing the Adoption of Web-Based Shopping: The Impact of Trust (Vol. 35, pp. 32-49): ACM SIGMIS Database.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. Electronic Commerce Research and Applications, 1, 247-263.

Suh, B., & Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. International Journal of Electronic Commerce 7(3), 135-161.

Tan, F. B., & Sutherland, P. (2004). Online Consumer Trust: A Multi-Dimensional Model. Journal of Electronic Commerce in Organizations, 2(3), 40-58.

Turner, C. W., Zavod, M., & Yurcik, W. (2001). Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites. Retrieved 4 March, 2007, from http://www.ncassr.org/projects/sift/papers/icecr01.pdf

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2005). Strategies for Building and Communicating Trust in Electronic Banking: A Field Experiment. Psychology & Marketing, 22(2), 181-201.

# Appendix A – Ethics Approval

# MEMORANDUM

## Auckland University of Technology Ethics Committee (AUTEC)

To: Brian Cusack
From: **Madeline Banda** Executive Secretary, AUTEC
Date: 24 September 2007
Subject: Ethics Application Number 07/169 **Impact of perceived security mechanisms on consumer trust in online banking transactions.**

Dear Brian

I am pleased to advise that a subcommittee of the Auckland University of Technology Ethics Committee (AUTEC) has approved your ethics application at their meeting on 17 September 2007. This delegated approval is made in accordance with section 8.1 of AUTEC's *Applying for Ethics Approval: Guidelines and Procedures* and is subject to endorsement at AUTEC's meeting on 8 October 2007. The subcommittee noted that the response to section E.7 of the application was inadequate and not at all related to the research in question. It all so added that the response to section B.1.8 in the EA8RA self assessment is misleading as AUT students will be intentionally recruited.

Your ethics application is approved for a period of three years until 17 September 2010.

I advise that as part of the ethics approval process, you are required to submit to AUTEC the following:

- A brief annual progress report indicating compliance with the ethical approval given using form EA2, which is available online through *http://www.aut.ac.nz/about/ethics*, including when necessary a request for extension of the approval one month prior to its expiry on 17 September 2010;
- A brief report on the status of the project using form EA3, which is available online through *http://www.aut.ac.nz/about/ethics*. This report is to be submitted either when the approval expires on 17 September 2010 or on completion of the project, whichever comes sooner;

It is also a condition of approval that AUTEC is notified of any adverse events or if the research does not commence and that AUTEC approval is sought for any alteration to the research, including any alteration of or addition to the participant documents involved.

You are reminded that, as applicant, you are responsible for ensuring that any research undertaken under this approval is carried out within the parameters approved for your application. Any change to the research outside the parameters of this approval must be submitted to AUTEC for approval before that change is implemented.

Please note that AUTEC grants ethical approval only. If you require management approval from an institution or organisation for your research, then you will need to make the arrangements necessary to obtain this.

To enable us to provide you with efficient service, we ask that you use the application number and study title in all written and verbal correspondence with us. Should you have any further enquiries regarding this matter, you are welcome to contact Charles Grinter, Ethics Coordinator, by email at charles.grinter@aut.ac.nz or by telephone on 921 9999 at extension 8860.

On behalf of the Committee and myself, I wish you success with your research and look forward to reading about it in your reports.

Yours sincerely

Madeline Banda
**Executive Secretary**
**Auckland University of Technology Ethics Committee**

Cc: Kritika Law Fqt8171@aut.ac.nz, AUTEC Faculty Representative, Design and Creative Technologies

## Appendix B – Questionnaire

# Security and trust in Online Banking Questionnaire

**Note:** Completion of the questionnaire will be taken as an indication of consent to participate.

**Instructions**

1. Tick one box to express your response to each statement [ ✓]

### Section 1: General Questions

1. Gender M [ ] F [ ]

2. Age < 20 [ ] 20-29 [ ] 30-39 [ ] 40-49 [ ] >50 [ ]

3. No. of years of Internet experience <1 yr [ ] >1yr [ ]

4. No. of years of Internet Banking experience <1 yr [ ] >1yr [ ]

| | | | | | | |
|---|---|---|---|---|---|---|
| **Section 2: Perception of Security**<br>The questions below are used to rate your perception and experiences when working with an online banking website | | | | | | |
| **1. I believe that the communication with the site is restricted to the website and me if** | | **Strongly Disagree** | **Disagree** | **Undecided** | **Agree** | **Strongly Agree** |
| a | I receive warning messages when the communication is insecure | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | The web browser does not show a padlock symbol | [ ] | [ ] | [ ] | [ ] | [ ] |
| c | The site address contains 'https' | [ ] | [ ] | [ ] | [ ] | [ ] |
| **2. I believe the communication between the website and me is tamper free if:** | | | | | | |
| a | The site does not indicate it is using encryption technology | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | I am warned if messages have been tampered with. | [ ] | [ ] | [ ] | [ ] | [ ] |

| | | | | | | |
|---|---|---|---|---|---|---|
| c | I am not informed if information in transit is deleted. | [ ] | [ ] | [ ] | [ ] | [ ] |
| **3. I believe that I am communicating with a secure website if:** | | | | | | |
| a | I can connect to the website in an acceptable time limit. | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | I can access the website for limited time in a day | [ ] | [ ] | [ ] | [ ] | [ ] |
| **4. I believe the website ensures that only I can access my information if:** | | **Strongly Disagree** | **Disagree** | **Undecided** | **Agree** | **Strongly Agree** |
| a | They ascertain my identity by requesting login information. | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | Additional methods of verification such as personal details are not requested. | [ ] | [ ] | [ ] | [ ] | [ ] |
| **5. I believe the website authorises transactions from my account only if requested by me if:** | | | | | | |
| a | I cannot view all information related to my transactions | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | The website verifies my identity before processing these requests. | [ ] | [ ] | [ ] | [ ] | [ ] |
| **6. I believe that the website will take responsibility for requests they process on my account if:** | | | | | | |
| a | The website provides a policy ensuring that they will take responsibility | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | The site does not provide evidence to prove it has sent a message to me. | [ ] | [ ] | [ ] | [ ] | [ ] |
| c | The site will provide evidence to prove it has received a transaction from me. | [ ] | [ ] | [ ] | [ ] | [ ] |
| **7. I believe all my personal information will not be misused if:** | | | | | | |
| a | The website does not provide information on the bank's privacy policies. | [ ] | [ ] | [ ] | [ ] | [ ] |
| b | I am aware of the exact nature of personal information that will be collected during a transaction. | [ ] | [ ] | [ ] | [ ] | [ ] |
| c | The site remembers information entered in previous transactions. | [ ] | [ ] | [ ] | [ ] | [ ] |
| | | | | | | |

<table>
<tr><td colspan="7"><b>Section 3:  Trust</b><br>The questions below are used to rate your trust when working with an  online banking website</td></tr>
<tr><td>a</td><td>I believe my transactions through the website are likely to be secure</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td></tr>
<tr><td>b</td><td>I believe my transactions with the bank will not be reliable</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td></tr>
<tr><td>c</td><td>The bank will inform me if there are problems with my transactions</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td></tr>
<tr><td>d</td><td>The bank keeps customers' best interests in mind</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td></tr>
<tr><td>e</td><td>I do not trust the online banking website.</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td><td>[ ]</td></tr>
</table>

***Thank you for participating!***

# Appendix C – Correlation Matrix

| | Mean | Std. Deviation | PC1 | PC2 | PC3 | PI1 | PI2 | PI3 | PAV1 | PAV2 | PAU1 | PAU2 | PAT1 | PAT2 | PNR1 | PNR2 | PNR3 | PP1 | PP2 | PP3 | T1 | T2 | T3 | T4 | T5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PC1 | 3.72 | .792 | 1.000 | | | | | | | | | | | | | | | | | | | | | | |
| PC2 | 3.18 | .976 | .350 | 1.000 | | | | | | | | | | | | | | | | | | | | | |
| PC3 | 3.44 | 1.011 | .354 | .610 | 1.000 | | | | | | | | | | | | | | | | | | | | |
| PI1 | 3.05 | 1.134 | -.062 | .123 | .128 | 1.000 | | | | | | | | | | | | | | | | | | | |
| PI2 | 3.10 | 1.093 | -.012 | -.024 | .043 | .516 | 1.000 | | | | | | | | | | | | | | | | | | |
| PI3 | 3.00 | 1.094 | -.079 | .156 | .212 | .525 | .513 | 1.000 | | | | | | | | | | | | | | | | | |
| PAV1 | 3.23 | 1.241 | .080 | .148 | .053 | -.110 | .028 | -.123 | 1.000 | | | | | | | | | | | | | | | | |
| PAV2 | 2.99 | 1.138 | .082 | .165 | .069 | -.088 | -.012 | -.018 | .682 | 1.000 | | | | | | | | | | | | | | | |
| PAU1 | 3.75 | 1.151 | .190 | .033 | .089 | -.171 | -.119 | -.126 | .055 | .097 | 1.000 | | | | | | | | | | | | | | |
| PAU2 | 3.03 | 1.224 | .157 | .046 | -.029 | -.088 | -.166 | -.141 | .030 | .114 | .554 | 1.000 | | | | | | | | | | | | | |
| PAT1 | 3.29 | 1.184 | -.327 | -.156 | -.208 | .007 | .019 | .006 | -.101 | -.116 | -.042 | -.016 | 1.000 | | | | | | | | | | | | |
| PAT2 | 3.70 | 1.121 | -.146 | -.040 | -.155 | .023 | -.112 | -.056 | .033 | -.031 | .018 | -.004 | .676 | 1.000 | | | | | | | | | | | |
| PNR1 | 4.00 | .826 | .127 | .019 | -.154 | -.162 | -.059 | -.184 | .052 | -.024 | .056 | -.067 | .070 | .082 | 1.000 | | | | | | | | | | |
| PNR2 | 2.98 | .945 | -.076 | -.153 | -.152 | -.112 | -.079 | -.066 | -.042 | -.007 | -.010 | -.026 | .227 | .110 | .505 | 1.000 | | | | | | | | | |
| PNR3 | 3.69 | 1.001 | .111 | -.183 | -.163 | -.141 | -.014 | -.124 | -.084 | -.082 | .045 | -.104 | .158 | .160 | .449 | .411 | 1.000 | | | | | | | | |
| PP1 | 2.99 | 1.258 | .188 | .094 | .032 | -.074 | -.060 | -.039 | .093 | .063 | .067 | .128 | -.314 | -.206 | -.073 | -.242 | -.182 | 1.000 | | | | | | | |
| PP2 | 3.05 | 1.089 | .035 | .020 | -.021 | -.008 | .047 | .102 | .081 | .080 | .077 | .192 | -.135 | -.055 | -.101 | -.301 | -.096 | .586 | 1.000 | | | | | | |
| PP3 | 2.97 | 1.224 | .218 | .055 | .035 | -.119 | -.105 | -.006 | .164 | .119 | .156 | .147 | -.208 | -.067 | -.022 | -.269 | -.113 | .610 | .564 | 1.000 | | | | | |
| T1 | 3.53 | 1.119 | .064 | .044 | .114 | -.073 | -.098 | -.080 | .023 | .146 | .232 | .060 | -.057 | .037 | -.025 | .036 | .119 | -.040 | .058 | .034 | 1.000 | | | | |
| T2 | 3.35 | 1.030 | -.048 | -.055 | .019 | .038 | -.017 | -.094 | -.079 | -.004 | .079 | .082 | .012 | -.014 | .080 | .145 | .060 | -.016 | -.050 | -.064 | .492 | 1.000 | | | |
| T3 | 3.46 | 1.026 | -.056 | -.045 | .058 | -.044 | -.054 | -.067 | .156 | .100 | .104 | .013 | -.034 | .029 | -.027 | .046 | -.068 | .091 | .080 | .089 | .455 | .365 | 1.000 | | |
| T4 | 2.40 | 1.000 | .045 | -.020 | .019 | -.049 | -.022 | -.125 | -.024 | .003 | -.045 | -.047 | -.033 | -.007 | .064 | .063 | .025 | .069 | .022 | -.009 | .312 | .343 | .234 | 1.000 | |
| T5 | 2.47 | 1.112 | .091 | -.024 | .068 | .001 | -.088 | -.137 | -.078 | -.111 | -.050 | -.061 | -.104 | -.019 | -.157 | -.072 | -.099 | .062 | -.083 | .072 | .176 | .193 | .207 | .456 | 1.000 |