CHAPTER - 1
CHAPTER 1

INTRODUCTION

The banking sector of any country occupies a prominent place in augmenting the all round development since it determines the economic pulse of a nation. This sector is interwoven with all the other sectors of an economy therefore, it is considered as the central nervous system or nerve center of the economy in meeting the national objectives. The sustained development in this sector establishes the high growth trajectory in all the spheres, in terms of financial and economic stability. The traditional banking system that have been adopted all over the world has resulted in the cost and time overrun which forced the banking sector to register the overall dismal performance. The huge public loss suffered by the Government of India in the hands of public sector banks has forced our Indian economic planners to insist upon showing at least an average performance. They sincerely felt that the public sector banks should also perform well for its survival though they are not primarily established for making profits. It is also felt that the persistent loss suffered in the hands of public sector banks in India could no longer be tolerated.

India’s access to globalization in the year 1991, as a result of a glorious effort taken by the world trade organization (WTO) in terms of economic liberalization and privatization that brought all the countries of world under common umbrella. The LPG process made all the countries of the world to play the role as a global village. The new globalized scenario has enabled the countries of the world to do business across the national frontiers, to which the Indian banking sector is not an exception. This environment in the Indian banking sector attracted more foreign direct investment (FDI) and the multinational banking companies to establish their banking business in India. The presence of foreign banks operating in India alongside the
Indian public sector banks has created a fierce competition. In this volatile situation, the public sector banks also forced to show a good performance for its sustainable development. The Indian economic planners advocated the privatization, in the event of any banking institution who could not perform well and make profit. It has also been suggested for the merger of non performing banks and open them to private operators. This situation has opened the way for multinational banking companies such as Standard Chartered bank, HSBC, RBS, Citi Bank, etc to serve the Indian public along with the existing public sector banks and private sector banks such as HDFC, ICICI, IDBI, in India. At the backdrop of the ongoing globalization process, the banking companies in India started marketing their technology driven financial products and services with a service edge and the service dimension of the banking institutions are enlarged, with a shift from traditional physical banking services system to virtual/digital banking service system.

Compared with traditional channels of offering banking services through physical branches, e-banking uses the internet to deliver the traditional banking services to their customers such as, opening accounts, transferring funds and electronic bill payments. E-banking can be offered into two main ways. An existing bank with physical offices can also establish an online site and offer e-banking services to its customers in addition to the regular channel through world wide web. Through this method, customers can access their bank accounts through the internet and in addition to the core e-banking services such as account balance enquiry, funds transfer, electronic bill payment, financial calculators, online stock quotes, brokerage services and insurance.

Generally, e-banking is provided without extra cost to customers who are attracted by the convenience of e-banking through the internet and the banks can operate more efficiently when customers carry out transactions by themselves rather than going to a branch physically. Without physical branches, net banking can cut
operating costs and can potentially offer high deposit rates to its customers and waive many fees normally charged by a bank with large network of physical branches. The world banking sector has been reaping the benefits of revolution in information and communication technology and the range of e-banking services is likely to increase in the future.

The internet has been existing since the late 1960’s but for most of that time it was only accessible to Governments and for scientific research purposes only. By the mid 1990’s as web interfaces improved, it became available to the public and e-commerce development allowing businesses to offer their products and services on the web. E-commerce became possible in early 1990’s when the internet was opened to commercial use. With the availability of the internet commerce websites round the clock, it has become very important to the users to trace and track the transactions, as they occur to ensure the account status and stability.

According to Kalakota and Whinston (1996), e-commerce has different definitions, From a communication perspective, it is the delivery of information, products/services or payments via telephone lines and computer networks. From a business perspective, it is the application of technology to improve the automation of business transactions and workflow. From a service perspective, it is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery. Consumers need a high quality service, Just In Time (JIT) service, and a faster, more secure and less expensive process. From an online perspective, it is the capability of buying and selling products and information on the internet.

Further, e-commerce is the purchase of goods or services (products, information, etc) through online transactions and the transfer of funds over computer networks (Olle, 2000). These activities occur between different parties with the
support of technology networks, (Kalakota, Whinston, 1996). In addition, the process of executing commercial transactions electronically with leading technologies such as Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT) and electronic mail support (EMS) and B2B commerce. These technologies also give people the opportunity to exchange business information and do business transactions electronically.

Besides, e-commerce involves buying and selling goods, purchasing and providing services, and making other financial transactions over the Internet (Poole, Lambert, Woodford, & Moschovitis, 2005). It also involves Just In Time transactions (JIT), which avoids the problems of internet bills costs. Therefore, ecommerce has reduced the cost of conducting some kinds of business and has made organizations more profitable even though it requires other costs to allow it to be established. The Internet and e-commerce finally have given the opportunity to the public to buy, sell, collect, and exchange information easily, securely, and quickly (Olle, 2000). With the Internet and e-commerce, the concepts of time and location have lost their importance because anyone can buy, sell, and do business from anywhere by accessing the Internet (Olle, 2000).

Physical banking has been the usual way that customers make use of a banking transaction and financial services which involves physical branches that are located around the most populated areas to serve their clients and allow people to complete their transactions and services in person (Sulaiman, C.H, and Wee, 2005). Virtual banking, which does not involve any physical action i.e., going to a bank building, standing in a queue, and face to face communication, exists in the form of ATMs, phone banking, home banking, and Internet banking. A virtual bank, in other words, is a non-branch bank (Kemal, 2001) that involves the provision of fully automated banking services. Online shopping has become available and more
convenient and secure because of the appearance of online banking (Poole, Lambert, Woodford, & Moschovitis, Iqbal & Molyneux, 2005).

Internet banks are the most important financial tools and services such as, ATM, telephone banking, home banking, internet banking, opening an account, accessing account information, electronic cheque conversion, transfer funds, bank statement, purchase bank products, download account information, pay bills, order check or deposit book, check reconciliation, change passwords, alerts, find locations of ATM, request a credit card or debit card, request a loan and check status, housing mortgage, stock information, tax documents and information, tutorials and online banking help, exchange and prime rates, digital signature, etc in the modern economy.

**Background of the Study**

The advent of multinational banking companies in India has posed a tremendous challenges not only to the banking public, online service providers but also to the banking institutions itself. Whether the banking public are particular about the reliability and the security of their banking transactions, it is the duty of the service providers and the banking institutions which provide the online services to plug the loopholes in the system and the technology. This guarantee would enable the users to have faith in the system and the early adoption and the continued usage. In this regard, the onerous task lies not only in the hands bankers and the service providers but also the user public. The service providers should imbibe faith in the technology that makes the user public readily accepting the adoption of online banking. The reliability of the technology shall evince faith in the system among the user public. The system so adopted should be user-friendly, hassle-free and fool-proof and should act as a watertight compartment in the event of any security breaches and the resultant risks and loss.
Besides, the present day bank customers are of two types, viz risk takers and risk averse. In both the cases, the ultimate loss lies with the bank customers. When they are at loss, they accuse the bankers, the system, the technology and the service providers. The cross accusation can be eliminated only when the security and risk concerns of the customers are convincingly addressed. Once the consumers are convinced and wrong perceptions towards risk and security issues are addressed, the adoption of online banking is easy. The risk in online banking are mostly resulting in risk of loosing sensitive financial information to the wrong hands and loss of money. The security issues are mostly relating to non-reliability of the system, system loopholes, system attack and manipulation. This would give away the chance for the wrong persons to intrude into the system. The security measures undertaken by the service providers and the banking institutions would enable the customers to adopt the online banking services.

The security attacks and vulnerability of attacks that are reported in the media, frequently is the reason behind for the reluctance of the users to adopt online banking services. Besides, the wrong perceptions of the customers towards security issues and risks factors pertaining to online banking are the reasons for non-adoption of online banking services. The unawareness relating to reliability of the technology is also one of the reasons for non-adoption of online banking services. When the accounts are subjected for risk and security threats, the privacy issues come into existence. There are certain vital and sensitive information which cannot be interchanged with others should be protected at any cost. When the system is subjected to security attacks, the privacy of the information is questioned.

The information privacy is meant for the customer himself and it aims at keeping away the enemies, rivals, adversaries and others whose motives are ill, shall be protected and the assurance can be given by the system developers, service providers, the institution which adopts the services for the benefit of the customers. If
there is any flaw in this respect, the customers’ belief in the system, technology and the institutions is totally affected. The trust factor is the utmost requisite of the online adopters, the mistrust in any system or in any technology or in any institution will cripple the online adoption permanently. These things relating to trust, risk, security and privacy are the major detractors for the early adoption of online banking services. The strenuous efforts to evolve a suitable control and preventive measures taken by the online service providers, technology developers and the institutions that provide online banking services, is the only way out for these problems.

**Online Banking Issues – An Overview**

Online banking (OLB) is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society. Online banking is also referred as Internet banking, e-banking, virtual banking and by other terms.

The issues relating to net banking services and its adoption are identified and grouped under four major categories, viz issues relating to trust factors, issues relating to risk factors, issues relating to privacy factors and issues relating to security factors.

**Trust related issues – Detrimental to online banking adoption**

Trust refers to an online users willingness to rely on a Web-based business or a Web-based bankers and to be vulnerable to the actions of a business whose positive outcomes are expected from the interaction characterized by uncertainty. Relationship marketing needs trust to enhance the adaptability to the changing dynamics of complex social organizations, such as the global market place (Morgan and Hunt, 1994) and downsizing situations (McNeilly and Lawson 1999). It helps the marketers
of services select proper marketing tools in customer relationship (Garbarino and Johnson, 1999). It is viewed as a crucial component in interpersonal relationships (Doney, Cannon, and Mullen, 1998 and McKnight et al., 1998) as a foundation for cooperation and teamwork and as a driving force for successful relationship marketing (Jap, Mnolis and Weitz, 1999 and Walter 1999).

It is a multi-dimensional construct that includes trust perception of the customer, trustworthiness of the business, trust in service providers and trust in technology. Trust of the customer using web based commerce is a psychological phenomenon that involves individuals perception, behavioural deviation, interpersonal relationship, understanding, faith, sensitivity, previous experience, intention and willingness towards online banking services. The trustworthiness of the business (banks) with whom the customer interacts for the banking services includes credibility (Rotter’s 1967, 1971 and 1980), reputation (Lewicki and Bunker 1995), integrity (Doney and Cannon 1997) and predictability (Bhattachartya et al., 1998).

The efficiency of the online service providers relies mostly on their capacity to instill faith in the information protection and the effective transmission and usage when needed without any chance of leakage of information to the hackers. Otherwise, the users will be reluctant to adopt online services. The technology that provides facilities to the users should be highly reliable and hassle free. If the businesses do not have enough mechanism to protect or prevent the online breach then it is utter failure for the both online customers and the bankers, since the buyers are already bombarded with negative stories about web based commerce, such as virus threat, identify thrift through public medias. The efficacy of the technology should be augmented by control mechanisms like, firewalls, passwords, TCP/IP address, Malware protection, etc to win the confidence of the customers.
Besides, a GVU survey (1998) conducted by the Georgia Institute of Technology, USA reported that more than half of offline customers claimed that lack of trust is one of their reasons for not registering with any Web sites (cited in Dayal et al., 1999). Web-based transactions require identification, which could generate new trails of personal data (Clarke, 1997). This reflects the weak trusting relationship between Web-based customers and the bankers especially when they have to give their sensitive information to the bankers and online service providers for the first time.

One way to increase the growth of Web-based commerce is to make the customers feel comfortable and secure in giving personal and/or financial information via a telecommunication network. Increased trust in a service provider and technology could help businesses develop and maintain effective relationships with their customers. In the initial trust relationship, the judgments of trustors or customers about the behavior or performance of trustees or business will be based on customer’s belief or perceptions rather than on experiential facts. The belief that other parties or business are trustworthy is based on the assessment of their benevolence, reputation, integrity and predictability (Mayer, Davis and Schoorman, 1995 and McKnight, Cummings and Chervany et al., 1998). These things are substantiated by the number of previous studies conducted by Doney and Cannon, 1997; Schurr and Ozanne, 1985; Sharma, Tzokas, Saren and Kyziridis, 1999 and Swan, Bowers, and Richardson, 1999 that examined the trust related issues among the users of online banking transactions.

Further, a key to success of B2C systems is certainly a wide customer adoption of technologies. Incorporating interpersonal communication via trust relationships into information systems also helps design effective Web-based commerce applications and business practices. The online customers’ perception in information exchange is a critical issue that has a significant contribution on the acceptance and adoption of Web-based commerce. This study attempts to identify the factors that
influence online customers’ trust, which is an important ingredient for system acceptance. Customer acceptance is a key factor for the growth of Web-based commerce. System designers include characteristics or factors that make online customers feel comfortable to engage in online banking. This study, therefore, approaches the challenges of online banking customers’ perception toward the threat of security and privacy by proposing a trust model. This model enables the pertinent parties to obtain a better understanding about customer’s perceptions and help online bankers or online businesses to promote the adoption of electronic commerce.

Risk perceptions – A predominant issue in online banking adoption

The Internet is not simply an another distribution channel for the financial institution’s products. Offering financial services on the Internet is not as simple as adding a new branch. Risk is the perception that the strength of the harmful event is greater than that of beneficial event. Conversely, risk is the subjective possibility of loss perceived by customer (Chiles and McMackin, 1996). Risk is present when customer are exposed to the probability of an adverse consequence (Worchel, 1979). In the development of a new exchange relationship, customers are forced to face risk (Davenport et al., 1999) for several reasons. It may be very tedious if not impossible or infeasible for customers to monitor businesses’ behaviors all the time. This invisibility could lead to dishonest behavior by the banks. Sheppard and Sherman (1998) indicated that this type of risk relies mostly on information asymmetries, which is the difference between the available information accessible or affordable by banks and by customers.

Moreover, if businesses misuse their customers’ sensitive information, customers assume the risk of indiscretion (Sheppard and Sherman, 1998), which is the risk that, for example, customers’ identities will be stolen or used against them.
Thus, trust laid a strong platform to alleviate against the risk of opportunistic behavior among stakeholders (Bigley and Pearce, 1998).

The willingness to assume risk, despite the freedom to accept or reject the risk, is vital to adopt online banking. The judicious acknowledgement and consideration of risk distinguishes the trust from related concepts, such as confidence and faith in the online banking system. Trust has been characterized in terms of acceptance of risk, and the existence of risk in online banking creates a need for trust. Therefore, trust serves to reduce and to increase risk taking. Trust between people and systems is predicated on technical competence. People can expect the systems to perform the technical tasks that they were designed for.

Individuals may respond to risk and ambiguity differently (Ghosh and Ray, 1997). The presence of ambiguity is often interpreted as risk but each individual customer perceives its accentuation differently. Customer may perceive Web-based commerce engagement as either an opportunity or threat. There might be two extreme types of customers: customers who do not worry about security until they experience a serious loss first-hand; and those who worry about everything they come across in the press and put up tight restrictions on Web-based trust that they cannot earn productivity gains. Risk perception is defined as the tendency of a customer to take or avoid risks (Mayer et al., 1995).

Risk is defined as a customers’ perceptions of the uncertainty and adverse consequences of engaging in an activity (Dowling, and Staelin, 1994 cited in Jarvenpaa et al., 1999). Making an online banking involves uncertainty and risk. The higher the level of perceived risk, the higher the level of trust is required to engender the willingness to engage in an online banking services. Conversely, trust increases the likelihood that a customer confer personal vulnerability. Therefore, a customer’s trust for an electronic services mitigates the risk perception. At the same time, the
amount of trust for the business will affect the perceived level of risk relating to technology and service delivery system (Jarvenpaa et al., 1999). In the Web-based commerce, a customer’s risk perception involves a belief about the likelihood of positive or negative outcomes pertaining to relationship with a Web-based business. Trust influenced the amount of risk the trustors who were willing to bear.

In other words, they proposed that if trustors' trust outweighed the threshold of their perceived risk, they will engage in the relationship, which was called risk-taking in relationship. McKnight et al. (1998) proposed that in the initial relationship, there was a link between trust and trusting intention, which corresponds to willingness to engage in an online banking. Therefore, this study includes risk perception as a trust outcome and as a moderator between trust and willingness to engage in an online banking.

Security perceptions – A crux of the issue in online banking

Perception and reality are not always the same. Perceptions on various aspects of Internet vary between individuals and this variation in consumer perception may have strong effect for online banking. The internet is convenient and simple to use because it provides them with control and convenience (Sheth & Sisodia, 1977). However, the technology on which the internet is based is not reliable. Users are not confident of security of their financial and personal information.

The principle problem that consumers face when buying on internet or fears concerned with security and privacy. Their fear is justifiable as their transaction information would be intercepted and used by someone else (Bush and Haris, 1998). Misuse or theft of personal information and computer hacking is found to be important in influencing users perceptions of web security and confidentiality. Therefore, security and privacy issues play a key role in individual perceptions of web.
purchases and e-business payment system. The credit card information is the next security concern in this aspect.

The second most important factor driving the security perceptions of the respondents related to their personal information being sold by firms to other internet companies or misused (Hurley & Ragothaman, 2000). Therefore, issues such as using reliable technology and securing financial and personal information are of major concern for internet users. Attitude towards technology are implicated as an important factor in many policy contexts. Risk is undoubtedly a factor in such attitude (Sjöberg, 2002). Therefore, consumer perceptions on online transactions and the risk involved have a significant impact on the adoption of online banking.

The consumers want to feel safe and comfortable. Thus, online banks have to work especially hard because they have to deal with both the reality and the perception of security. The reality is that while there is a potential security problem surrounding any online transactions, the banks have to deploy adequate security to protect the customers and themselves. The perception, however, is that transmitting personal information such as credit card numbers over the internet is dangerous, that hackers lurk everywhere, and that personal information is being sold by firms to other internet companies or misused.

**Privacy and its implications on online banking adoption**

Web based commerce ensures highly promising growth in terms of numbers of internet users and online businesses, its revenue and the volume of transaction to business to business (B2B) and business to consumers (B2C). Business to Business (B2B) commerce, such as Electronic Data Interchange (EDI) has been viewed as a pre-cursor of electronic commerce among the businesses. The internet is widely used among the businesses so as to enable the companies to communicate each other
electronically through private communication networks called value added network, public internet and network for corporate use only (Intranet) or for use by companies and its business partners (Extranet). While the B2C commerce requires buyers to transmit their sensitive information, such as name, address, credit card number over the internet, which is a public infrastructure.

The internet retail business has realized that it is difficult to convert online users or shoppers into first-time online buyers, instantly. The customers major threats are derived from concerns about information security and privacy. **InterMarket Group (1999)** reports that major hurdles claimed by internet users are concerns about credit card security and privacy, which are considered as the most commonly cited barriers. Another reason cited for not engaging in web-based transactions are the concern over insecure communication and untrustworthiness of the vendor (**Furnell and Karweni (1999)**). Consumers are fearful or reluctant to provide their personal or credit information over the internet since the perceived lack of security and the fear of being scammed (**Dinnie, 1999**). They do not know who will retrieve that information without their consent. Therefore, web based commerce needs to assure their buyers that no unauthorized people can fraudulently enter the vendor’s electronic commerce system or impersonate them in order to steal their money and ensures that all the transactions are authentic one. Therefore, online banking users are to be assured with making secured transactions and ensuring the control over the privacy of their personal information.

Besides, the threat of online fraud is one factor that inhibit the online users or customers from engaging in digital transactions since identity theft and breach of personal or sensitive information are also the major concerns. The threats of electronic commerce partly arise from computer capabilities of storage and retrieval, any-to-any connection, ubiquitous access and use, fast interaction, and the computer intelligence to provide levels of personalization. The web-based buying context tends
to rely more heavily on understanding the buyer’s personalities, their beliefs, and their expectations of businesses’ behavior. The findings of some previous research helps to obtain a better understanding the perceptions in a brick-and-mortar or physical branch environment, which may or may not be applied to an electronic environment. It also provides them with considerations about security and privacy levels, which should have a proper balance between perceived risk and convenience. It enables system designers to integrate technological, business and behavioral perspectives together when they design Web sites in order to make customers feel comfortable when exchanging their sensitive information.

Customers’ attitude towards adoption

The users attitude towards online banking is measured with the help of the customers voluntariness, the relative advantages such as opportunities to enhance efficiency, reduced cost, improved communication and improved information delivery attached with online banking, the compatibility of the various kinds of transactions to the user public, ease of use and perceived usefulness. Besides, the adaptation of any internet technology relies heavily on the user’s perceptions, skills, abilities and expertise in internet application. It also heavily depends on how clear the results are, how easy it is to attribute results to the innovation and what hurdles are in the way of the communication of those results.

Need and Importance of the Study

E-banking encompasses an array of financial transactions, once done through the tangible exchange of information, now are done electronically. While the benefits of such advancements have been welcomed, there also have been drawbacks. Issues such as security, fraud and theft have deterred people from participating in the Internet and e-banking revolutions. Furthermore, without the proper countermeasures
in place to prevent malicious actions, users may find the prospect of Internet banking unappealing. The problem therein arises; with technology’ revolutionizing effect on banking procedures, improper security measures prevent customers from enjoying the benefits. Besides, the security issue extends beyond simply deterring participation; it extends to the improper use and manipulation of the Internet for illegal gain and illegal activities. But everyone and anyone can be at risk from malicious users.

Furthermore, from the perspective of the institution offering the service, the security issue can be a major obstacle to traverse in the marketing of these online services to customer. Banks, nowadays devote considerable time and assets in perfecting their online services and to have them not taken advantage due to Internet insecurity can prove very costly. While society has drifted away from these ideals, there are still those who do not believe in banking institutions and those who, for example, refuse to carry credit cards. To these individuals, cash is the safest way to carry out transactions, leaving little room for fraud or other such illegal and harmful activities. In addition to the hesitation of parting with one’s money, there has been mistrust in banking institutions. Since these debilitating events, banking institutions have taken considerable measures to ensure a tragedy of this magnitude does not happen again. By forging relationships and establishing a sense of security and faith in their customers, banks have rebuilt their credibility.

Credibility may not be enough to bridge the gap between banking and e-banking services. A sense of security is easier to sell when the transaction is taking place in front of the person whose funds are being used. The proposition of e-banking in a secure environment is more difficult for older generations to relate to, especially those who are accustomed to tangible transactions. The inability to use a personal computer due to lack of know-how can be the case with an indiscriminate number of people. Also, financial status can be a hindering factor due to the cost involved in owning a personal computer. Not only does the computer need to be purchased, but
also it needs to be guarded with the proper tools to prevent malicious attacks, viruses, and other illegal activities.

An inexperienced user with a shaky understanding of computers may find the change to online banking overwhelming. If there are enough of these types of users, the online banking industry will fall victim the technology obstacles, which are inherent to any e-banking system. Feeling safe enough on the Internet to conduct these financial transactions represents a host of security concerns associated with the ideas mentioned above. The psychological barriers involved across demographic characters of the users in terms of gender, age, financial status (income), occupation and level of education in relation to an individual’s comfort level with electronic commerce present a foundation to the security dilemma and may provide a correlation for current attitudes towards e-banking adoption.

**Problem focus and justification for the study**

The success Mantra of marketing of any product or service is winning the confidence of the consumers, to which the banking industry is not an exception. Once the confidence or the trust of the consumers is developed and established, then the marketer is successful in his mission. But winning the confidence of the customer is an arduous task which involves so much of complexities. The trust issue may be relating to trust of the users, trust in the system and technology, trust in service providers and trust in institutions that offer online banking services. The facility of accessing involves furnishing of information relating to the customers which are exchanged with service providers, bankers and the outside agencies in a restricted way, is a compelling factor in any online mode of transactions, in terms of ATM, telebanking, personal banking, etc. This situation creates the mistrust and hesitation among the customers to use Internet banking services offered by banks which leads to leakage of sensitive personal information.
The internet is the public domain whereby geographical boundaries are eliminated. Cyber crimes are therefore, difficult to identify and control. In order to promote internet banking services, it is necessary that the proper security infrastructure is made. The internet provides a new and inexpensive channel for banks to reach out their customers. It allows the customers to access bank facilities round the clock. The highly unregulated internet provides a less than secure environment for the banks to interface. The diversity in computer, communication and software technologies used by the banks increases the challenges, facing the online bankers. It is the duty of the bankers to convince and ensure the reliability of the security system of internet banking. The purpose of the computing network is sharing of computing resources and data across the whole organization and the outside world. Though the security measures are guaranteed by the system developers, service providers and the banking institutions, security breaches are often reported. These things create a fear among the banking public that their personal information relating to the accounts may fall in wrong hands.

A major driving force behind the rapid spread of internet banking all over the world is its acceptance as an extremely cost-effective delivery channel of banking services as compared to other existing channels. However, the regulators and the supervisors all over the world are concerned about different types of risks and their controllability. Because of rapid change in information technology, there is no finality either in the types of risks or their control measures. Both evolved continuously which includes operational risk, security risk, reputational risk, legal risk, money laundering risk, cross border risk, strategic risk, etc, it means internet banking carries various risks that hamper the usage, useful innovation and experimentation.
The aim of computer security is to preserve computing resources against abuse and unauthorized use and to protect the data from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed systems. These things require authentication, access control, data confidentiality, data integrity, non-repudiation and security audit trail, which are to be guaranteed by the people involved in the internet banking system as a whole. Any flaw in the above aspects result in breach of privacy of the individual customer and the hesitation for non- adoption of online banking services, as reported in journals, newspapers and research works.

Against this background, the present study attempts to develop the following research question and examines empirically, how the above aspects pertaining to trust, security, risk and privacy are impacting the adoption / non-adoption of online banking services across the select sample respondents belonging to different demographical classifications such as age, gender, income, occupation and educational background?

Scope of the study

The trust is a multi-dimensional construct supplemented by theories of psychology, social psychology, sociology and economics. We need more than one dimension to better understand how trust is engendered. Levels of trust and trustworthiness depends on knowledge or information about businesses behaviour and predictability of their future behaviours. Trust is also a kind of attitude or perception based on individual differences and the expected positive outcomes. In web-based commerce, providing sensitive information through the internet could be viewed as risky activity. Besides, trust is needed when one party is fearful that another party will act opportunistically.
With regard to security issues, a business realizes the secured system particularly foolproof system are not available yet. Customers fierce about these issues need to be alleviated in order to encourage them to make use of online services. There insecurities are also enlarged by the stories or news about internet fraud and the threats from the computer hackers. Besides, the most frequently cited reasons for not becoming involved in online transactions is the fear of online fraud which covers the threat from security issues. In a web based commerce environment, users cannot control or monitor every action that businesses will take regarding their information.

Risk is defined as the customer’s perception of the uncertainty and adverse consequences of engaging in an online activity. The higher the level of perceived the risk, the higher the level of trust is required to endanger the willingness to engage in an online transactions. Three basic sources of risk are security failures, data misuse and reliability. The online banking is more risky than traditional banking hence, security has become a top priority. Offering financial services on the internet is not as simple as adding a new branch. The willingness to assume risk, in spite of the freedom to accept are reject the risk, this vital to adopt online banking. The level of risk in online transactions depends on reliability of technology and its acceptance, users technical competence, unauthorized access or use, hacking, encryption and vulnerability.

There is a hue and cry among the online customers upon the leakage of customers personal data to other parties. Customers have to send their personal and financial information over the internet which is a public infrastructure. Banks could also get to their customers’ information and store it for future use with or without customer’s permission. Such secondary use of information is also a major concern. Customers are also bombarded with negative stories about web-based commerce such as virus threats and identity threat. Confidentiality, integrity and authentication are the measures to address the above concern of maintaining the secrecy of the personal
information. Any deficiencies in these aspects would result in mistrust and privacy encroachment.

Therefore, it is an imperative to examine the role of trust in the perspectives of expectations, willingness, risk taking, vulnerability to opportunistic behaviour, uncertainty environment, trust propensity, third party assurance and reputation. The role of risk in terms of willingness to acceptance, users technical competence, unauthorized access, hacking, encryption and vulnerability. The role of security in terms of technology, reliability, informational quality, etc and the role of privacy in terms of protective measures and Information pass on request and their implications on the adoption of online services, are carried out in this research.

**Objectives of the study**

1. To study the conceptual issues and to review the literary background pertaining to trust, security, risk and privacy factors in the adoption of online banking, in general and its relevance to Indian context, in specific.

2. To identify, study and analyse the variables relating to the trust and risk factors that influence the adoption of online banking services.

3. To analyse the various aspects of security and privacy factors that determine the adoption of online banking services.

4. To measure and critically evaluate the combined effect of trust, security, risk and privacy factors across the sample respondents belonging to different demographic classifications viz, gender, age, income, occupation, educational background and type of bank with reference to various online banking services provided by the sample banking institutions under the study.

5. To suggest immediate and long term measures for the enhanced trust, confidence and willingness to adopt the online banking services.
Limitations of the study

1. The area of the study is restricted to Chennai Metro only.

2. The present study is restricted to the select sample size of respondents, public and private sector banks under the study.

3. Traditional banking services are excluded from the purview of this research.

4. The finding of this research is purely based on the opinion of the sample respondents upon the various online banking services offered by the sample banking institutions, under this study

5. The suggestive measures have policy implications of the government and the banking organizations that provide net banking services.

Research Methodology

This study has adopted both descriptive and analytical methodologies. The adoption of descriptive methodology has become a compelling factor in this research as it reviews the theoretical background and the conceptual issues pertaining to online banking (net banking) services. The adoption of analytical methodology is also considered as an imperative since it measures and analyses the associations and degree of variance between the independent and dependent variables that influence the online banking adoption across the sample respondents using various net banking services offered by some select banks, under the study. Besides, the design of the study comprises of data source, determinants of online banking service adoption, sample size, and sampling procedure, development of questionnaire as a tool for data collection and the scaling technique, analytical framework and the statistical tools adopted for data analysis.
Sources of data

The data source for this study is primary, collected directly from the sample respondents by serving them a structured questionnaire. In addition, the use of secondary data has also been made in this research, wherever necessary which are supplemented by text books, journals published in and outside India pertaining to online banking and the publications of RBI covering various aspects of online banking services.

Instrument for data collection

The data collection method adopted for this study is a survey method, using a structured questionnaire covering the distinguished aspects, viz trust, risk, security and privacy that influence the online banking adoption, with five responses, whose weights are ranging from strongly disagree (1), to strongly agree (5), under the five point scaling technique suggested by Rennis Likert. The questionnaire is designed in such a way that meets the various requirements of the objectives set and pursued in this research.

Sample size and sampling procedure

The sample size for this research is seven hundred respondents selected at random, covering different demographic characters, viz gender, age, educational background, income level and occupation, using various online banking services with reference to the four determinants that influence the online banking adoption. These sample respondents using online banking services have been served with the structured questionnaires in person. Out of the original sample size, only six hundred
and one filled questionnaires have been received back representing approximately 86%. Out of the six hundred and one filled questionnaires, fourteen questionnaires were found to be incomplete. Hence, the final sample size for this research is 587. The renowned authors on research methodology across the globe such as Zigmond and Uma Sekaran suggest any sample size more than five hundred would be an ideal sample for larger studies, despite the authors on statistics like S. P. Gupta and others insist upon only any sample size less than thirty as small and above thirty as large sample size. Hence, the adoption of five hundred and eighty seven sample size for this study can be reasonably justified.
## Table 1.1 showing the sample size and sampling procedure

<table>
<thead>
<tr>
<th>ONLINE BANKING SERVICES</th>
<th>GENDER</th>
<th>AGE</th>
<th>INCOME</th>
<th>EDUCATIONAL BACKGROUND</th>
<th>CUSTOMER / OCCUPATION</th>
<th>TYPE OF BANK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Male</td>
<td>Female</td>
<td>&lt;20</td>
<td>&lt;21-30</td>
<td>&lt;31-40</td>
<td>&lt;41-50</td>
</tr>
<tr>
<td>E-PAYMENT (DEBIT &amp; CREDIT CARD)</td>
<td>37</td>
<td>31</td>
<td>2</td>
<td>15</td>
<td>17</td>
<td>14</td>
</tr>
<tr>
<td>ELECTRONIC FUND TRANSFER</td>
<td>39</td>
<td>32</td>
<td>0</td>
<td>15</td>
<td>16</td>
<td>19</td>
</tr>
<tr>
<td>MOBILE BANKING</td>
<td>27</td>
<td>30</td>
<td>15</td>
<td>17</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>ONLINE TRADING</td>
<td>36</td>
<td>30</td>
<td>15</td>
<td>17</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>E-RESERVATION</td>
<td>31</td>
<td>27</td>
<td>17</td>
<td>15</td>
<td>13</td>
<td>17</td>
</tr>
<tr>
<td>E-FILING</td>
<td>26</td>
<td>16</td>
<td>0</td>
<td>12</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>E-STATEMENT/REQUISITION</td>
<td>31</td>
<td>24</td>
<td>4</td>
<td>11</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>E-INVESTMENT PURCHASE AND SALE</td>
<td>29</td>
<td>21</td>
<td>0</td>
<td>11</td>
<td>16</td>
<td>14</td>
</tr>
<tr>
<td>ELECTRONIC CLEARANCE SERVICES</td>
<td>35</td>
<td>31</td>
<td>0</td>
<td>17</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>TOTAL</td>
<td>326</td>
<td>261</td>
<td>61</td>
<td>142</td>
<td>156</td>
<td>152</td>
</tr>
</tbody>
</table>

Source: Primary Data
Pilot study (Pre-testing)

Before carrying out the final research, the pilot study was carried out on restricted sample i.e., 10% (70 samples) of the original sample size, selected at random, covering different demographic characters of the respondents, using different online banking services, as a pre-testing measure. The absolute aim of this process is to verify the reliability and validity of the statements incorporated in the research instrument, the scale development and to ensure the internal consistency. Hence, the Cronbach Alpha’s test was carried out on the samples for making suitable modifications, if any. The Alpha value is found to be (0.85) which validated the instrument and its reliability, directed the researcher to carry out the final study.

Research variables incorporated and the justification

The present day customers are not only rationalists and analysts as well. They analyse the various aspects of the product or service in different angles before they actually buy the product or avail the service of their choice. Different aspects of the product or service are vital and significant to individual customers at different point of time. No single factor is the very important factor for a customer to choose a particular product or service. Many factors play a conflicting role during pre and post purchase or adoption. Also, the purchase behaviour differs from person to person depending on distinguished purchase environment and their respective likes and dislikes. Hence, the customers are forced to reckon with very many factors for their adoption decisions as all the determinants have some role to play. Therefore, the problem of understanding the attitude of the present day customers towards a service is more complex in nature, because of their varied
concerns in terms of trust, risk, security, privacy, and behavioural deviations. In this context, the detailed and extensive review of literature that was carried out for this research has facilitated the present researcher with such standard variables that influence the adoption of online banking services across the globe. Hence, it has become an imperative to reckon with these standardized variables of the adoption of online banking services, can be reasonably justified. The variables that have been incorporated in this research, for further analysis, are detailed as follows.
**Table 1.2 showing the classification of variables that determine the adoption of Online Banking Services**

<table>
<thead>
<tr>
<th>TRUST FACTOR</th>
<th>RISK FACTOR</th>
<th>SECURITY FACTOR</th>
<th>PRIVACY FACTOR</th>
<th>ADOPTION / REJECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trust in systems and its complexities</td>
<td>• Users technical competence</td>
<td>• Security architecture</td>
<td>• Authentication protocol</td>
<td></td>
</tr>
<tr>
<td>• Trust in technology</td>
<td>• Unauthorized access/use</td>
<td>• Technical security</td>
<td>• Digital signature</td>
<td></td>
</tr>
<tr>
<td>• Trust in an electronic medium</td>
<td>• Security breach</td>
<td>• Internet security</td>
<td>• User identification</td>
<td></td>
</tr>
<tr>
<td>• Third party assurance (service providers)</td>
<td>(Hacking/interception)</td>
<td>(Transmission Control Protocol &amp; Internet Protocol)</td>
<td>• Certification authority</td>
<td></td>
</tr>
<tr>
<td>• Banker’s trustworthiness (Reputation, Integrity, Benevolence)</td>
<td>• Encryption</td>
<td>• Firewall</td>
<td>• Shared access to view websites</td>
<td></td>
</tr>
<tr>
<td>• Trust in Information (quality, reliability and credibility)</td>
<td>• Security failures</td>
<td>• Buggy software</td>
<td>• Password</td>
<td></td>
</tr>
<tr>
<td>• Demonstrability and visibility</td>
<td>• Data misuse</td>
<td>• Virus infected executables</td>
<td>• Biometry</td>
<td></td>
</tr>
<tr>
<td>• Familiarity and previous positive experience</td>
<td>• Vulnerability</td>
<td>• Identity theft</td>
<td>• Information pass on request</td>
<td></td>
</tr>
<tr>
<td>• Trust Propensity of the customer</td>
<td>(Hackers and Virus)</td>
<td>• Downloadable applets</td>
<td>• Online relationship</td>
<td></td>
</tr>
</tbody>
</table>

**Source: Primary Data**
Research Unit

India’s access to the globalization process has been witnessed with flooding of multinational banking companies into the Indian banking sector. The advent of foreign banks in the Indian banking industry created the massive expectations among the Indian customers as these banks market their technology driven products with a service edge to woo the banking public. As a result, the alarming bell is given to the indigenous bankers to shift their traditional banking services to online mode that results in the existence of fierce competition among the players in the Indian banking industry viz, private sector banks, public sector banks and foreign banks. This trend has posed a tremendous challenges to the bank customers and the banking companies for the successful implementation and adoption of online banking service. The technology adoption has become an arduous task for both the users and the service providers to create the trust among the adopters in terms of risk and security. In this context, the researcher has made a sincere attempt across the respondents selected at random OLB services of select private sector banks, public sector banks and multi-national banking companies.

Justification for area of the study

The area for this research is restricted to Chennai. Chennai metro as a capital of Tamil Nadu is consisting of population with multi-racial, multi–lingual, multi-cultural and multi- religious background. The urban Chennai has a wide spectrum of population with all socio-economic classification such as, different age groups, income groups, educational groups, occupational groups and social status, using different online banking services. Being Chennai as one of the metropolitan cities, houses the branches of almost all the private, public and foreign banks. Therefore, it has become convenient for the present researcher to select Chennai as a study area,
not only to minimize the cost and time significantly but also to have a ready sample respondents across various demographic classifications for the data collection, can be reasonably justified.

**Formulation and testing of null hypotheses**

Since, this study is an attempt to analyse the unknown area of the customer online banking service adoption behaviour, the formulation of Hypotheses has become an imperative. Besides, the association or not between the independent and dependent variables that influence the online banking adoption across the sample respondents with respect to different demographic characters may not be the same. The association and the degree of variance upon these demographic characters and the determinants of online banking adoption are tested with the help of the following null hypotheses.

**Null Hypothesis 1:** There is no association between different gender groups and the determinants of online banking adoption

**Null Hypothesis 2:** There is no association between different age groups and the determinants of online banking adoption.

**Null Hypothesis 3:** There is no association between different income groups and the determinants of online banking adoption.

**Null Hypothesis 4:** There is no association between educational levels and the determinants of online banking adoption.

**Null Hypothesis 5:** There is no association between occupation/users and the determinants of online banking adoption.
Null Hypothesis 6: There is no association between customers of different types of banks and the determinants of online banking adoption.

Null Hypothesis 7: There is no significant impact of trust factor on OLB adoption.

Null Hypothesis 8: There is no significant impact of risk factor on OLB adoption.

Null Hypothesis 9: There is no significant impact of security factor on OLB adoption.

Null Hypothesis 10: There is no significant impact of privacy factor on OLB adoption.

Analytical framework

The entire analytical processes of this research has a main focus on identifying the influence of the four factors, viz trust, risk, security and privacy that are responsible for the adoption of online banking services. It is arranged in three parts. The first part analyses the aspects of trust and risk factors that influence the adoption of online banking transactions. The second part analyses the issues relating to security and privacy factors that determine the adoption of online banking services. The third part of the analysis measures and critically evaluates the impact of these four factors viz trust, risk, security and privacy in the adoption of online banking services across the sample respondents belonging to different demographic characters viz, gender, age, income, occupation, educational background and type of bank. The absolute aim of this process is to measure the combined impact and to identify the association or variance of these factors with respect to different demographic characters of the respondents and to generalize the findings of this research.
Tools for data analysis

The second objective and third objectives of this research analyse the influence of various aspects pertaining to trust and risk related issues and security and privacy related issues, separately in the adoption of online banking services offered by the sample banks under this study. In this attempt, this study has employed the well known branch of multi-variate techniques of factor analysis using principal component analysis and varimax rotation that follow cluster analysis and discriminant analysis as a data reduction technique. The absolute aim of this process is to identify the factor weights and the intensity of the influence of these factors in determining the online banking adoption. In pursuing the fourth objective that measures the combined impact of four factors on adoption across the different demographic profiles of the sample respondents. The use of chi-square test, ANOVA, t-test, beta-coefficient and multiple – regression analysis have also been made to identify the association, variances and to test the null hypotheses, set for this study using SPSS version 20.0. In addition, these statistical tools are supplemented by descriptive statistics such as mean, standard deviation to cross verify the inferences made. The AMOS version 21.0 has been made to develop a new research model using Structural Equation Modeling (SEM) that reviews the combined impact of dependent (Adoption) and independent variables (trust, risk, security and privacy).
Chapterization

The report of this study is organized in seven chapters. The first chapter introduces the subject matter, discusses its background, the research problem, the need and importance and the scope. It also sets the objectives, limitations and outlines the research methodology adopted in this research.

The second chapter covers the extensive review of literature relating to the conceptual issues and the theoretical background pertaining to online banking adoption, elaborately.

The third chapter succinctly traces the global and Indian scenario pertaining to banking industry and the genesis, growth and dimension of online banking services over the years.

The entire analytical processes that have been carried out in this study are arranged in three chapters viz, four, five and six.

The fourth chapter details the results of analysis carried out to measure the impact of trust and risk factors.

The fifth chapter analyses the impact of security and privacy factors that influence the online banking adoption.

The sixth chapter combines all the four factors viz, trust, risk, security and privacy that influence the overall adoption or rejection of online banking services, the association and variances of these factors with respect to different demographic characters of the respondents. It also develops the research model that combines the factors of online banking adoption or rejection.

The seventh chapter summarizes the present research, highlights the findings and the conclusion drawn. It also suggests the immediate and long term measures to overcome the lapses identified in this research.