Chapter – 1

INTRODUCTION
Chapter – 1

INTRODUCTION

1.0 Introduction

The internet has brought about revolutionary changes in the life of modern man. It is impossible to explain in a few words the bewildering variety of services rendered by internet to various aspects of human life. Its application in financial service is just one amongst the many services rendered by internet. Utilizing the Internet for banking transactions securely is the main theme of research reported in this thesis. In particular, it is intended to evaluate the most essentially needed ‘Security and Its Standards’ for internet banking viz. e-banking.

Here, a few words about the internet would be appropriate. The internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite, like Transmission Control Protocol/Internet Protocol (TCP/IP), to serve billions of users worldwide. It is a network of networks with global scope and belonging to millions of private, public, academic, business and government entities. These networks are interlinked with the help of an array of latest electronic and optical networking technologies. The internet carries a vast array of information resources and services, most notably, the inter-linked hypertext documents of the World Wide Web (www) and super fast network enabled communication system which primarily capacitates e-banking. Security and confidentiality of transactions are the basic expectations of such complex network communication systems.

The success of e-banking depends upon familiarity, acceptability and accessibility of internet services to the common man. The projected estimates indicate that the worldwide internet user population would reach 2.6 billion by the end of 2015\(^1\). According to Internet Worlds Stat web site, the present scenario depicts that Asia scores the highest global online percentage (44.8%), followed by Europe (22%) and North America (12%)\(^2\). However, considering the density of population of each region, the internet penetration rate of Asia (26.2%) is very much less compared to North America (78.6%)
and Australia (67.5%). The internet penetration of Asia is still very much lower compared to the world’s average (32.7%) though it is higher than Africa (13.5%). With the development of IT infrastructure in the world there is a phenomenal growth in the internet services in Asia. These internet services has been driven by the financial and healthcare sector. The financial sector comprising of banking, insurance and stock market has benefited the most due to growth in internet technology since last 25 years. The advent of Java programming language in 1989 and high speed networks has enabled the adoption of internet services throughout the world in all the service sectors.

1.1 Banking in India

Banking in India dates back to 1786 when the General Bank of India was established. Subsequently Bank of Bengal (1809), Bank of Bombay (1840) and Bank of Madras (1843) were established as independent units and called it Presidency Banks. Later in 1920, the above three banks were amalgamated to form Imperial Bank of India. As a central banking authority to supervise the banking in India, the Reserve Bank of India was established in 1935. In 1955 the Imperial Bank of India was renamed State Bank of India and made as the principal agent of RBI to handle banking transactions of the Union and State governments all over the country according to the Banking Regulation Act, 1949.

In 1969, 14 major commercial banks were nationalized to extend the banking facilities to rural and semi-urban areas in the country. The Dr. C. Rangarajan Committee Report on Mechanization in Banking Industry was considered as a blueprint for mechanization and computerization of banks in 1984 and was the first step towards computerization of Banks. In 1991, the M. Narasimham committee recommended the liberalization of banking practices. Accordingly, the country witnessed the adoption of Information Technology with several foreign banks entering banking sector in India.

The internet penetration (% population) in India is only 10.2% as compared to China- 35.4%, Japan-80% and Malaysia-61.7%. As on December 2011, 121 million users were using internet in India. According to RBI, 40% of population has bank accounts. About 791.38 millions have mobiles, but of which only 157 millions do not have bank accounts. The first
Automated Teller Machine (ATM) was introduced in the year 1967 by Barclays Bank in Enfield Town in North London and was conceptualized by Mr. John Shephard-Barrons of Scotland and Mr. James Goodfellow was credited with introducing an encrypted card and Personal Identification Number (PIN). The first ATM in India was installed in 1987 by HSBC bank for its Sahara Road Branch, Andheri East in Mumbai. E-banking was introduced in India in 1993 with ATMs by foreign banks in 5 metropolitan cities. In 2007, fifteen biometric ATM machines were installed in five districts in southern India. The biometric ATM scanner kiosks scan user fingerprints rather than the user swiping a card and inputting a PIN number as in non-biometric ATM machines. The ATM’s are precursor to online banking / e-banking.

1.2 E-Banking

Banks and financial institutions are service organizations, operating within regions/ countries. As we move from the traditional ‘Paper and Pen’ to computers system in banking to store, process and communicate data, the consumers are benefited with faster and accurate transactions with privacy and security of data. Due to the phenomenal growth of IT in the last 15 years, the financial transactions through banks became easier and faster. It has also become an integral part of people in the country. E-banking or Internet banking has become the order of the day in reaching bank account holders through internet in office and homes.

1.3 Traditional Banking versus E-Banking

In spite of the many facilities offered by E-banking, bank customers still trust traditional method of banking and are reluctant to use online banking due to fear of data security breach. U.S. consumers reported losing more than $559.7 million from online fraud in 2009, up from $264.6 million in 2008, according to data released by the FBI.

Internet-based frauds jumped 33 per cent in 2008 over the previous year, causing a loss of 5 million dollars to the victims, with the fifth largest number of complaints coming from India, according to an FBI report. In 2009, Internet fraud losses from banks in India was ₹ 6.6 crores. Even though
internet fraud have increased, electronic banking benefits outweigh disadvantages of traditional banking system. In fact internet transactions can save money for its customer. ‘Stop payment’ done through electronic banking will not cost any extra fees but when done manually through the branch, the bank may charge the customer upwards of `50 per cheque plus the service tax. Through electronic banking, user can check transactions at any time of the day, and as many times as the user desires.

On the other hand, in the traditional method, the customers get quarterly statements from the bank and request for a statement at required time; it may turn out to be an expensive affair. The branch may charge `25 per page, which includes only 30 transactions. Moreover, the bank branch could take eight days to deliver.

If a fund transfer has to be made to a place where the bank does not have a branch, the bank would demand outstation charges. But, with the help of online banking, it will be absolutely free. The Internet and Mobile Association of India’s report on online Banking 2006, lists many advantages of online banking. It is convenient; it isn’t bound by operational timings; there are no geographical barriers and the services can be offered at a miniscule cost.

ATM/Debit card usage is growing in India. According to a report in the Business Standard which cited card trade publication, the Nilson Report, transactions made with both debit and credit cards in India grew 103 percent, i.e., $4.2 billion in 2002, with debit accounting for $3.5 billion of the total. About 95 percent of debit card transactions are ATM cash withdrawals, according to another Business Standard report.

Automated Teller Machines (ATMs) have gained prominence as a delivery channel for banking transactions in India. Banks have been deploying ATMs to increase their reach. As at the end of December 2007, the number of ATMs deployed in India was 32,342. The number of ATMs connected to National Financial Switch (NFS) being operated by National Payments Corporation of India (NPCI) just over 75,178 by March, 2011. According to a survey by Banknet India, 95% people now prefer this modern channel to traditional mode of banking. Almost 60% people use an ATM at least once a week. The number of ATMs per million people is as low as 18 units. The total number of ATMs in India, a country of 1.21 billion people, has increased
approximately by 30% in 2008 to 44,671\textsuperscript{11} and 80% of ATMs was installed in urban areas. By contrast, in the United States with a population of only 305 million people, ATMs number peaked at 395,000 in 2005 and in 2009 no of ATM grew to 4,03,000. It is expected that the demand for ATMs in India is expected to grow at 18% by 2013.

Debit cards in India are primarily used for ATM withdrawals to support cash-based transactions. In 2008, banks added 237 million debit cards. The number of debit cards at the end of February 2008 stood at 99.6 million as against 75.8 million as of April-end 2007 according to RBI sources. As on March 2009, number of credit cards circulation was 24.4 and 137.4 million debit cards respectively. The Chinese have spent nearly $24.0 billion using credit cards in 2008 compared to $6 billion in India. According to Visa research report, only 28% of “affluent” Indians have credit cards.

Due to introduction of these plastic cards the hackers and fraudsters have became very active and proficient technically, leading to increased bank frauds. The cyber frauds like data theft, denial of service attacks, credit card theft etc., has become the main source of financial threat to all the banks issuing credit/debit cards.

1.4 Cyber Frauds

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. This loss may be caused by

- Altering computer input in an unauthorized way.
- altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions
- altering or deleting stored data
- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Due to apprehension about data security and increase in cyber frauds at banks, the E-banking has made little progress in the Indian subcontinent. In the US there has been a 1534% increase in cyber frauds from 2000 to 2008
and increase of 33.1% from 2007 to 2008. From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions. This was a 22.3% increase as compared to 2008. The financial loss due to cyber frauds mainly from check fraud, no delivery fraud, confidence fraud, auction fraud and credit/debit card.

In India banks across the country have lost `6.6 crores through internet fraud with 233 incidents of cyber crime and the state of Tamil Nadu topping the list in 2009. Due to large increase in credit/debit card fraud in India, fraud in the banks are being monitored by RBI. The vigilance committee by Reserve Bank of India (RBI) was set up to set security guidelines to all the Banks in India.

The RBI’s mobile payment guidelines 4.1 says the technology used for mobile payments must be secure and should ensure confidentiality, integrity, authenticity and non-repudiation. From time to time the RBI issues guidelines to safeguard credit/debit card holders data privacy. Despite this, due to lack of understanding of technology and security standards by the user and the banks, cyber fraud has grown.

To make security robust, high secured network with the latest security measures is being implemented throughout the world. Two factor authentications are in vogue in any financial transactions validity. An authentication factor is a piece of information and synonymic for the process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Two-factor authentication (T-FA/2FA) is a system wherein two different factors are used in conjunction to authenticate transaction. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three methods: "something you know" (e.g., password or PIN), "something you have" (e.g., smartcard or token), or "something you are" (e.g., fingerprint or iris scan). Still robust and highly secured is the three factor authentication i.e. more than two factors, is being considered though it is quite expensive for implementation. The standards were developed for conducting financial transactions through internet. Banks are being pursued to follow Basel II standards, an international business standard that requires financial
institutions to maintain enough cash reserves to cover risks incurred by operations for maximizing its transactions and its usefulness to its customers. Similarly after offering E-banking, banks have to protect customer’s data and provide security on the internet. For credit/debit card transaction Payment Card Industry-Data Security Standard (PCI-DSS) was imposed to conduct transactions on the internet.

1.5 Data Protection

Around the world, data protection and privacy legislation is becoming increasingly important and a crucial part of overall IT Governance. It is in this field, in particular, that new IT laws are emerging on a regular basis. These IT laws were enacted by US and European countries to protect customer data.

16 Key Legislations


US: Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Senate Bill 1386 (SB-1386), the Fair Credit Reporting Act (FCRA) and various State Breach Laws.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (which took effect in 2003) is a set of federal standards that requires healthcare organizations (Covered Healthcare Providers, Health Plans and Healthcare Clearing houses) to implement security standards that protect (and keep up to date) patient data and to standardize on electronic data interchange.

The Gramm-Leach-Bliley Act (GLBA), also known as the "Financial Services Reform Act of 1999" requires US financial institutions to establish administrative, technical and physical information safeguards to ensure the confidentiality and integrity of customer records and information.

The Senate Bill 1386 (SB-1386), also known as the California Information Practice Act, was passed into law in July, 2003. The primary purpose of the bill is to force companies to think more seriously about information security and its impact on the residents of California.
Canada: The Personal Information Protection and Electronic Documents Act (abbreviated PIPEDA or PIPED Act) is a Canadian law relating to data privacy. It governs how private-sector organizations collect use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents.

European Union: the Data Protection Directive (implemented slightly differently in each of the EU countries) - and the EU Safe Harbor regulations which enable US companies to escape prosecution under EU regulations. Many of the legislations enacted by different countries overlap or contradict existing laws and for few of them there aren’t any detailed regulatory implementations guidelines or meaningful case law. Hence unified approaches to have common regulations were framed.

The IT Unified Compliance Framework

The Unified Compliance Framework (UCF) is the first and largest independent initiative to map IT controls across international regulations, standards, and best practices. The UCF accomplishes its goal by harmonizing terms and controls against the backdrop of a master hierarchical list.

Some of the compliance frameworks and standards that many organizations have to grapple with include:

- US's Sarbanes-Oxley Act
- US's Health Information Portability and Accounting Act (HIPAA)
- Control Objectives for Information and Related Technology (COBIT)
- Gramm-Leach-Bliley Act (GLBA)
- ISO 27001
- ISO 27002
- Business Continuity Institute (BCI),
- Standards from the British Standards Institute (BSI),
- Information Security Forum (ISF),
- PCI DSS
The UCF has given way to development of information security standards to protect the customer data and maintain non-disruptive financial transactions in banking and financial institutions.

1.6 Information Security Standards

ISO (International Standard Organization)\textsuperscript{17} / IEC (INTERNATIONAL ELECTRO-TECHNICAL COMMISSION)\textsuperscript{18} 27001:2005 (usually known just as ISO 27001) is the best practice specification that helps businesses and organizations throughout the world to develop a best-in-class Information Security Management System (ISMS)\textsuperscript{19}. BS10012 (British Standards) provides specifics on developing a Personal Information Management System to comply with data protection legislation.

International Organization for Standards (ISO)\textsuperscript{20} 27001 is the first in a family of International Information Security Standards that will underpin and protect IT worldwide.

ISO 27001 is designed to harmonize with ISO 9001:2008 and ISO 14001:2004 so that management systems can be effectively integrated, implements the Plan-Do-Check-Act (PDCA) model and reflects the principles of the 2002 OFFICE OF EXCHANGE COORDINATION AND DESIGNATION (OECD) guidance on the security of information systems and networks. To protect the credit/debit card holder’s data major five card issuing banks in US, UK and Japan together came out with a standard called PCI-DSS.

1.6.1 Payment Card Industry-Data Security Standard

In January 2005, the world’s five leading payment card brands - American Express, Discover Financial Services, Japan Credit Bureau (JCB)\textsuperscript{21}, MasterCard and Visa collaborated to create a worldwide standard for protecting consumer cardholder data.

The Payment Card Industry (PCI) Data Security Standard (DSS) was updated in October 2008 and revised in September 2010, a compilation of best practices for securing data throughout the information lifecycle. The PCI standard identifies several core IT security technologies, as well as various processes and procedures, required to protect cardholder data.
The introduction of the PCI DSS has revolutionized security within the e-commerce industry with respect to the way in which credit card data is handled and stored. E-commerce activity is immeasurably safer today than it had been without PCI DSS.

However, PCI DSS compliance alone does not guarantee the service or the credit card data that the service origination may be storing within its system is completely immune from risk of being compromised.

The PCI DSS is a complex set of rules and requirements that applies to every person, business or organization that handles credit/debit card data. This includes any person, business or organization that receives, stores, processes or transmits credit/debit card details.

The PCI DSS is a product of the Payment Card Industry Security Standards Council (PCI SSC), an organization founded by participating payment brands Visa International, Master Card, American Express, Diners Club and JCB.

The purpose of the PCI SSC is to establish a uniform World Wide standard to aggressively address vulnerability and risk associated with the handling of credit card data across all Industries.

The official definition of whom and what is now required to have PCI DSS compliance is:

"PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply".

Therefore, if website touches the PAN (Primary Account Number) which is usually the 16 digit credit card number itself in any way, even if it is only to transmit it directly to a 'real time' payment gateway, or perhaps to store it in some way, then online Business (website) must be PCI DSS compliant certified in its own right. The applicable PCI DSS criteria are as follows:

**Level 1** - Visa and MasterCard World Wide transactions totaling 6 million and up, per year, and any merchants who experienced a data breach.

**Level 2** - Visa and MasterCard transactions totaling 1 million to 6 million per year.
**Level 3** - Visa and MasterCard e-commerce transactions totaling 20,000 to 1 million per year.

**Level 4** - Visa and MasterCard e-commerce transactions totaling 1 to 20,000 per year.

The vast majority of all those businesses or organizations operating e-commerce websites on the internet today fall into the Level 4 classification. PCI compliance is not a request, or suggestion, it is now a requirement and is enforceable.

Any person, business or organization that qualifies into any of the above compliance levels but is found not to be compliant with PCI DSS, risks not being allowed to handle cardholder data and possible heavy fines (up to $0.2 million) and penalties which could be levied on a monthly basis.

### 1.6.1.1 Mapping out PCI DSS Compliance for Organization

PCI DSS Compliance is not an overnight process; rather, it's the collaboration of numerous initiatives undertaken by various personnel within the organization, all working towards a common goal. In short, it can sometimes be a monumental effort needed by all for ensuring PCI DSS compliance is ultimately successful. So, where to begin, what's needed from the user and organization, and where do find the tools and resources for undertaking PCI DSS compliance?

Outlined are key activities, deliverables, and milestones for ensuring the organization is on the right path for PCI DSS compliance.

**Phase I: PCI DSS Readiness Assessment**

**Phase II: Remediation & Implementation for PCI DSS**

**Phase III: Assessment & Reporting for PCI DSS**

### 1.6.1.2 Phase I: PCI DSS Readiness Assessment

If an organization is new to PCI DSS compliance, then it is wise to begin the process with a Readiness Assessment which helps pave the way toward successful compliance by undertaking the following activities:

- In-depth scoping analysis as it relates to the PCI DSS criteria and its 12 core areas.
Review and analysis of current policies, procedures, and initiatives throughout the organization for meeting PCI DSS compliance.

Analysis of debit/credit (i.e., payment) Card "Transaction Environment" Analysis of hardware/software systems, components and all other related application and network layer devices.

Identifying and analyzing all significant third party outsourcers and managed service providers used by the organization.

Internal assessment of available personnel within the organization.

Cursory, initial walk-through of all 12 core PCI DSS standards necessary for meeting compliance.

1.6.1.3 PCI DSS compliance requirements

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized: They are

*Build and Maintain a Secure Network*

Requirement 1 : Install and maintain a firewall configuration to protect cardholder data

Requirement 2 : Do not use vendor-supplied defaults for system passwords and other security parameters

*Protect Cardholder Data*

Requirement 3 : Protect stored cardholder data

Requirement 4 : Encrypt transmission of cardholder data across open, public networks

*Maintain a Vulnerability Management Program*

Requirement 5 : Use and regularly update anti-virus software

Requirement 6 : Develop and maintain secure systems and applications

*Implement Strong Access Control Measures*

Requirement 7 : Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

**Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security

**1.6.1.4 Phase II: Remediation & Implementation for PCI DSS**

Immediately after the completion of a PCI DSS Readiness Assessment, it is important that organizations take corrective action on any deficiencies or weaknesses found that may serve as a roadblock for successful PCI DSS compliance. Generally, one of the areas of concern is that of documented policies and procedures. While most organizations are very good at what they do, they simply lack many of these much needed policies and procedures that are so vital to PCI DSS compliance. Thus, the development of a companywide "Corporate Security Policy & Procedure" Handbook for helping meet the demands as set forth for PCI DSS compliance is essential. NDB Advisory of US - Specializing in providing clients with scalable, efficient solutions for meeting the rigorous demands of Payment Card Industry (PCI) compliance can assist in helping develop these documents, creating highly customized policies and procedures for the company.

In addition to the policies and procedures, additional recommendations may be given on any number of topics or issues regarding PCI DSS compliance, such as adding, removing and modifying application and network layer devices, enforcing additional security procedures, or a host of other requirements. And because each entity has different needs and requirements that are based on a number of parameters, it’s more proof of why a Phase I PCIDSS Readiness Assessment is considered crucial.
In short, the remediation and implementation phase is a vital element for ensuring that your organization meets the rigorous demands set forth for PCI DSS compliance.

1.6.1.5 Phase III: Assessment & Reporting for PCI DSS

The actual PCI DSS assessment is not a standalone process that starts from scratch. Rather, it is a collection of efforts continued from the Readiness Assessment and the implementation phases. All the time and effort put into Phases I and II have prepared the organization for the assessment and all testing and validation activities that accompany it. Upon completion of the PCI DSS assessment, there are a host of reporting and deliverable requirements necessary for final confirmation of successful PCI DSS compliance. Reporting and submittal of compliance can become complex, as there are a number of different protocols to follow. The PCI DSS Qualified Security Assessor (QSA) will help assist and guide banks on these administrative matters. To assess the impact of PCI DSS on security of credit/debit cardholder’s data, surveys were conducted between 2006 to 2009.

1.6.2 PCI-DSS 1.1, 1.2 – summary changes from 1.1 to 1.2

PCI DSS 1.2 is considered a minor update to the DSS version 1.1. PCI DSS 1.2 has the same 12 requirements as did 1.1 and no new requirements have been added. The intent of 1.2 is mainly to clarify the existing requirements and provide some flexibility in terms of interpretation of the standard.

Segmentation of network, although not a requirement, the council provided guidance around scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.

Scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.
The changes are made to counter the growing number of violations of PCI-DSS. These changes were made according to feedback from the merchants, service providers and banks. The main changes are as follows.

- Segmentation of network helps isolate cardholder data environments and provide better controls.
- Wireless networks should be implemented using industry best practices like IEE 801.11X.
- Web application security is mandatory
- Firewall audit for 6 months (90 days in 1.1)
- Annual visit to offsite storage and review and acceptance of security policy annually.
- Announcement of Quality Assurance (QA) program for assessors.
- Documentation of cardholder data environment.

PCI-DSS 1.2 is largely focused on securing the perimeter to stop cyber criminals from getting in. There is a desire to have more requirements to addressing the internal threat.

1.6.3 PCI-DSS 2.0 summary changes

The latest version of the Payment Card Industry Data Security Standard (PCI DSS v2.0) came into effect on January 1, 2011. In this version, one year has been given to comply with the new standard. If a company started a Report on Compliance (RoC) assessment cycle in 2010 using v1.2.1, that cycle can be completed before the end of 2011 against v1.2.1. If an organization starting a new assessment in 2011, the RoC will be based on v2.0 but that doesn’t mean a significant change from previous assessments. The reason for this is that the overwhelming majority of changes between the previous and new version of the standard are clarifications.

The PCI Security Standards Council defines “Clarifications” to the PCI DSS as follows – “Clarifies intent of requirement. Ensure that concise wording in the standards portray the desired intent of requirements.” Of the 137 changes detailed in the Summary of Changes from PCI DSS Version 1.2.1 to 2.0, 119 of them are typed as clarifications. The purpose of the clarifications is to lower the points of contention during audit with better, more precise wording in the standard.
1.7 Research Methodology

To evaluate security standards adopted by Indian banks offering credit/debit cards facility questionnaires were developed. A simple questionnaire with 25 questions (Appendix-VI & VII) was used at first; this yielded responses that varied greatly—and were often vague and required extra work on the part of researcher to gain clarification. In addition, at some banks, the questionnaire was handled by people who were reluctant to provide statements that would imply that security was an issue.

The researcher contacted many other banks to gather more data. This required a different, streamlined approach, and decided to build an online questionnaire (www.surveymonkey.com) based upon earlier responses to elucidate more accurate information. The criteria in this questionnaire are based upon existing standards that are readily available, either in print form or on the Internet. The criteria were based on well-known accepted industry practice.

Methodology of the study employed are analytical user surveys and verbal interviews. It is very difficult to collect security related data from banks by an outsider. From 2003 to 2009 survey was conducted on 76 Indian banks comprising of national, public, private and foreign banks. Only 32 banks responded due to the nature of the survey.

The direct interview method was adopted to get more authentic information. The interviewed people were System administrators/ Security auditors/Management of banks for collecting sensitive security information. The data was also collected through secondary sources such as web sites, books, CDs, journals, reports, magazines and newspapers. The user responses from credit/debit card holders, a survey of credit card holders – Offline/Online was conducted. About 325 responses were collected during 2006 to 2009.

To elucidate more information and authenticate the data, the researcher also studied and analyzed the reported cyber frauds from 2002-2010 in banking and financial institutions in India.
1.8 Scope of the Study

The scope of the research is limited to evaluation of online security standards such as PCI DSS in the banks offering credit/debit cards in India and develop a security model. The researcher has conducted the survey at 76 Indian banks. The data was collected from 2003 to 2009, to evaluate potential security measures and adoption of security standards in online banking transactions.

1.9 Organization of the Study

The study was conducted from 2003 and the data was collected from secondary sources- research, finance, and IT Security and banking journals. The three questionnaires were designed to get data from i) Banks, ii) User, and iii) IT Professionals.

These questionnaires were sent to 76 private, public, cooperative and foreign banks with self addressed stamped envelope and initially only 12 banks responded. Only banks which were issuing credit card and debit card were selected for the survey. To get more data, direct interviews were conducted with General Manager-IT of Syndicate Bank, Karnataka Bank, Corporation Bank, State Bank of Mysore, SBI, Vijaya Bank, AXIS Bank, ICICI Bank and HDFC bank in person, via phone and e-mail. In 2008, the questionnaire was redesigned to get data regarding adoption of PCI-DSS in banks through online (www.surveymonkey.com). The email was sent with a request to answer the online questionnaire to 61 banks. Only 20 banks responded positively and were compiled. Totally 32 banks were involved in the offline and online survey and data was entered into statistical package – SPSS for compilation and analysis of research data. Also the debit/credit card user survey with a questionnaire was conducted from 2007 to 2009. About 325 debit/credit card users from all walks of life were surveyed to get feedback regarding the use of credit / debit card, ATM and online banking. Using SPSS, the data collected were compiled and analyzed.
1.10 Objectives of Study

The basic objective of the study is to understand and evaluate the security standard PCI-DSS adopted by Indian banks offering credit/debit cards. The above primary objective can be sub divided into the following specific objectives:

1. To ascertain the impact of online banking in Indian banks and study how effectively Indian banks have adopted to e-banking and its impact on its performance.
2. To study the existing various security metrics and develop new metrics to measure security.
3. To evaluate the impact of security standard PCI-DSS on online banking.
4. To study the effect of regulatory bodies and cyber laws on reducing the cyber frauds.
5. To study the technology to be adopted in carrying out smooth and secured online banking.