CHAPTER - I
CHAPTER-I
“INTRODUCTORY”

1.1 INTRODUCTION

Banking system is one of the oldest businesses systems in the world and retained its existence from ancient times in India. The banking system has its source in the earlier centuries. Awareness of banking was there among the prehistoric society because they felt the necessity of banking and makes use of money transaction to get proper benefits. The importance of banking system was recognized by the people because they had realized the value of money in their life.

Present banking system plays a significant role in the society. Banks are considered as the most trustworthy institution in administrating the money matters. Banking is the only system, which provides security to cash when deposited in the bank, which provides cash as and when required and even safe guards from fraudulent money tenders. No financial monetary transactions are possible without the help and support of the banks. Banks are considered as the most reliable and responsible institution in managing the finances and money matters. A banking organization is the key to economic growth and development.

The bank nationalisation of 14 major banks has laid down the foundation of banking reforms in India. The period from 1969 to 1979 is known as the post nationalization period of banking and explains how the reforms in banking sector have lead to the expansion of commercial banks and their branches all over the country. Bank credit was made instrumental for economic development of the country by way of spreading the banking habit among the people under the scheme of ‘Social Control’ of banks.

Government took major steps in the Indian Banking Sector Reform after independence. In 1955, Imperial Bank was nationalized and merged to form State Bank of India. Seven banks forming subsidiary of State Bank of India was nationalized in 1960. On 19th July 1969 nationalization of 14 major banks was carried out. Second phase of nationalization
was carried out in 1980 with six more banks as a policy decision under Indian Banking Sector Reform. In the early 1990s, the then Narasimha Rao government concentrated on a policy of liberalization, licensing a small number of private banks.

In the last thirty years, India's banking system has achieved several outstanding successes. The most important is its approach to the people standing in the last row. Banking system is no longer restricted to metros and urban centers in India. In fact, Indian banking system has reached to the unbanked rural centers of the country. This is one of the main aspects of India's growth in bank’s branches.

Expansion of Commercial Bank’s Branches since Nationalization (1969-2012)

Table 1.1: Expansion of Commercial Bank Branches since Nationalisation (1969-2012)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Commercial Banks (including RRBs &amp; LABs)</td>
<td>73</td>
<td>272</td>
<td>182</td>
<td>173</td>
</tr>
<tr>
<td>No. of Bank Branches of which Rural and semi-urban bank offices</td>
<td>8,262</td>
<td>60,570</td>
<td>74,563</td>
<td>1,01,261</td>
</tr>
<tr>
<td>Population per office</td>
<td>64,000</td>
<td>14,000</td>
<td>15,000</td>
<td>13,000</td>
</tr>
</tbody>
</table>

At the time of nationalisation i.e. In 1969, presence of commercial banks in India were only 73 with 8,262 branches comprises of 1503 branches in Metro centers, 1584 branches in Urban centers, 3342 branches in Semi-urban centers and 1833 branches in Rural centers. During the time span of 1969 to 2012, there was an absolute growth of 94.38% in terms of increase in number of commercial banks in India As on March 2012 total number of commercial banks were 173 with 101261 branches comprises of 17396 branches in Metro centers, 21804 branches in Urban centers, 25705 branches in Semi-urban centers and 36356 branches in Rural centers all over the country.

To keep the pace with the process of liberalization in banking sector and globalization of banking services, the economic and financial sector reforms were introduced in India. Due to implementation of economic and financial reforms speedily resulted in the creation of an efficient and competitive banking system in India.

1 www.rbi.org.in (2013)
Indian banks consist mostly of Scheduled commercial bank (SCBs), which includes both Public Sector Banks, and the Private Sector Banks. In Public Sector Banks, stake of government must be 51%.

The adaption of Information Technology in banking was planned by the landmark report of Dr. Rangarajan Committee (1984) and the signing of the settlement on computerization with Bank Unions in 1987. Establishment of second Rangarajan Committee, Saraf Committee, Shere Committee and the Vasudevan Committee had paved the way for computerization in the banking sector. As a result of the implementation of the recommendations of these committees, all Indian banks entered into the era of inter-bank & intra-bank connectivity of their branches and by accepting the recommendations on computerization all large branches of banks have been computerized.

Application of Information Technology was successfully administered in the banking system. Maximum banking transactions were done through information technology. Therefore it is concluded that information technology is the trouble shooter of the banking industry and also most helpful for the customers for their day to day banking transactions. Phone Banking, Automatic Teller Machines (ATM), Credit Cards, Debit Cards, ATM Cards, Smart Cards, Electronic Funds Transfer (EFT), Shared Payment Network System (SPNS), Electronic Clearing Services (ECS), Point of sale [POS] terminal, D-Mat Accounts, Electronic Data Interchange (EDI), E-Cheques, Computerized Accounting, E-Mail and RBI Net are some of the examples of administration of Information Technology in the Indian banking system.

It is pertinent to note that Information technology does not know physical boundaries and it made communication possible in any part of the world between the persons. These technological improvements have made the changeover possible from paper to paperless transactions in banking. Therefore, traditional banking shifted to electronic banking popularly known as e-banking. In the recent past, the banking transactions have become easier and faster as all the functions are started doing with the help of electronic medium. Specific areas where information technology widely used in the banking system are preparation and posting in ledger (LAN), portfolio management,
funds management, funds transfer, on-line banking credit appraisal, foreign exchange transaction, opening of letter of credit, issuance of letter of guarantee, preparation and submission of financial statements and last but not the least is the identification of fraudulent credit card transactions.

ATMs were introduced to the Indian banking industry in the early 1990s initiated by foreign banks. Followings are figures of growth of ATMs of Scheduled Commercial Banks in India.

**Growth of ATMs of Scheduled Commercial Banks in India (2005-2013)**

<table>
<thead>
<tr>
<th>Year</th>
<th>FY05</th>
<th>FY06</th>
<th>FY07</th>
<th>FY08</th>
<th>FY09</th>
<th>FY10</th>
<th>FY11</th>
<th>FY12</th>
<th>FY13</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of ATMs</td>
<td>16750</td>
<td>21509</td>
<td>27088</td>
<td>34789</td>
<td>43651</td>
<td>60153</td>
<td>74743</td>
<td>95688</td>
<td>114364</td>
</tr>
<tr>
<td>% Growth</td>
<td>--</td>
<td>28.41%</td>
<td>25.93%</td>
<td>28.42%</td>
<td>25.47%</td>
<td>37.80%</td>
<td>24.25%</td>
<td>28.02%</td>
<td>19.5%</td>
</tr>
</tbody>
</table>

ATM technology was initially started as a policy to defeat the inability of the banks by reaching to the customers at a minimum transaction costs and offering comfortable banking services. Since then, improvements in ATM technology and customer acceptance have also increased tremendously. Public sector banks have also joined the competition for expansion of ATM networks. Development of ATM networks is not only controlled for reducing the transaction costs, but also as successful promotional channel for marketing of the banking services.

The implementation of new technology in banking industry and advancement of e-banking not only offered opportunities for the customers to avail comfortable banking services and for the banks to expand banking business but has also gave an equal opportunities and opened the doors for new criminal activities. The technology that facilitated bank and its customers to perform business more effectively also provided the opportunities of globally organized criminal networks. Due to advancement of information and communication technology the entire world is transformed into a global

---

2Source Report on Trends and Progress of Banking in India, RBI, Mumbai, Various Issues
village but at the same time it put a serious threat to the existing and established banking institutions known as “Cyber Crimes”.

The development of Information Technology (IT) introduced the cyber space wherein internet made available equal opportunities to all the people to access any information and data storage. Due to increase of internet users, misuse of technology in the cyberspace was take hold of cyber crimes at the domestic and international level. “Cyber crime” is an criminal activity committed by using the computer or other electronic devices or Internet as the medium, in violation of existing enactment for which punishment is awarded as per the statute of the country.

The global nature of computer technology presents a challenge to the nations in the world to address Cyber crime. Domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate Cyber crime statistics because many of the incidents were not reported and many of the incidents were even not detected.

Cyber crimes are increasing globally and India too has been witnessing a sharp increase in cyber crimes in the recent years. Reserve Bank of India (RBI) regarding year wise and amount wise fraud cases in Scheduled Commercial Banks every year through publications in RBI Bulletin and on its website

The statistics published by the Reserve Bank of India (RBI) as of 31st March, 2013 in respect of Scheduled Commercial Banks relating to Cyber Crime cases of frauds and amount involved therein Year wise and slab wise as under.
Commercial Banks- Year wise Fraud Cases and Slab-wise Amount Involve

Table1.3- Commercial Banks-Year wise and Slab wise Amount Involved

<table>
<thead>
<tr>
<th>Amount</th>
<th>FY</th>
<th>No. of Cases</th>
<th>&lt; Rs 1 lakh</th>
<th>&gt; 1 lakh and up to Rs 1 crore</th>
<th>&gt; Rs 1 cr and up to Rs 50 crore</th>
<th>&gt; Rs.50 crore</th>
<th>Total Fraud Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pre 2004</td>
<td>2292</td>
<td>4.25</td>
<td>819</td>
<td>96.65</td>
<td>613</td>
<td>2951.64</td>
</tr>
<tr>
<td></td>
<td>2004-05</td>
<td>7553</td>
<td>12.50</td>
<td>2407</td>
<td>287.32</td>
<td>111</td>
<td>584.89</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11395</td>
<td>18.63</td>
<td>2334</td>
<td>290.20</td>
<td>192</td>
<td>1009.23</td>
</tr>
<tr>
<td></td>
<td>2006-07</td>
<td>20415</td>
<td>31.22</td>
<td>3048</td>
<td>325.02</td>
<td>158</td>
<td>791.17</td>
</tr>
<tr>
<td></td>
<td>2007-08</td>
<td>17691</td>
<td>30.25</td>
<td>3381</td>
<td>383.98</td>
<td>177</td>
<td>662.31</td>
</tr>
<tr>
<td></td>
<td>2008-09</td>
<td>19485</td>
<td>33.85</td>
<td>4239</td>
<td>442.94</td>
<td>214</td>
<td>1129.56</td>
</tr>
<tr>
<td></td>
<td>2009-10</td>
<td>20072</td>
<td>30.36</td>
<td>4494</td>
<td>474.04</td>
<td>222</td>
<td>1129.28</td>
</tr>
<tr>
<td></td>
<td>2010-11</td>
<td>15284</td>
<td>26.09</td>
<td>4250</td>
<td>494.64</td>
<td>277</td>
<td>1515.15</td>
</tr>
<tr>
<td></td>
<td>2011-12</td>
<td>10638</td>
<td>19.05</td>
<td>3751</td>
<td>509.18</td>
<td>327</td>
<td>213.23</td>
</tr>
<tr>
<td></td>
<td>2012-13</td>
<td>9060</td>
<td>22.11</td>
<td>3816</td>
<td>491.13</td>
<td>372</td>
<td>2798.00</td>
</tr>
<tr>
<td>Total</td>
<td>133885</td>
<td>228.31</td>
<td>32539</td>
<td>3795.10</td>
<td>2663</td>
<td>14684.46</td>
<td>11202.25</td>
</tr>
</tbody>
</table>

Fraud cases reported cumulatively by Commercial Banks as of 31/03/2004 to the tune of 3737 and amount involved therein to the tune of Rs.4296.80 crore. Whereas no. of cumulative cases reported by the Commercial Banks as of 31/03/2013 to the tune of 169190 and amount involved therein to the tune of Rs.29910.12 Crore. During the span of nine years i.e. from 2004 to 2013 Commercial banks reported the growth in number of cases to the tune of 165493 and growth in amount involved therein to the tune of Rs.25613.32 crore.

To curb & control the crimes arising out of the Internet & Computer Technology the different countries have enacted the specific legislation as per their requirement. The Information Technology Act 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162, on 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step towards the Law relating to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. Different types of cyber crimes have been explained as offences under Chapter IX. Several crimes related to banking and disclosures of information by organizations have been described in detail.

---

3 http://www.rbi.org.in
The IT Act, 2000 provides for the constitution of the Cyber Regulations Advisory Committee which has been advising the government as regards to any rules or for any other purpose connected with the act. The Act also has Four Schedules, the last one being the glossary and others which amend The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers’ Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the Act\(^4\). Currently, the IT Act, 2000 has been amended by the Information Technology (Amendment) Act, 2008. This law provides the legal infrastructure for Information Technology in India. The said Act along with its 90 sections is to be conceived with 23 rules called the IT rules, 2011

The present research work is the critical analysis of the impact of cyber crimes on the e-banking in India. Up to what extent the banking industry is affected by cyber-crimes like spreading viruses and worms, Trojan horse attacks, website compromise and malware propagation, denial-of-Service attacks (DDoS) and distributed denial of service attacks (DDoS), phishing or vishing attacks, hacking, spamming, network scanning/probing, cyber money laundering, fiscal frauds and other offences. This study is an effort to find out up to what extent IT Act, 2000 & IT Amendment Act, 2008 are effective and efficient enough for controlling the cyber crimes against e-banking in India. It is also an earnest effort to bring to the surface up to what extent the existing other laws (new and old) in India support to control cyber crime against e-banking in India.

The results of this study may prove to be helpful in assessing the effectiveness of the legislation, their weaknesses and will suggest ways to amend and plan for the future. These recommendations may go a long way in nurturing the academic appetite of teaching institutions, banks financial institutions and police machinery and also the judicial fraternity. The measures suggested by this study may be proved to be helpful in legal control of cyber crimes against e-banking in India in an effective way

\(^{4}\) The Gazette of India, Extraordinary part -2
1.2 STATEMENT OF THE PROBLEM

Banking industry has gone through major changes in recent past. Almost all the banks in India have adopted Information Technology solutions for rendering the banking services to their customers by using the IT tools & techniques to fulfill the needs of the customers. Due to the dawn of e-banking, conventional banking has been disappeared from the Indian banking scenario and banks have shifted from traditional banking to Core Banking Solution. Under these circumstances Indian banking industry is facing the challenges of impact of technology on the banking. In the age of information technology the swift expansion of, telecommunications, computers and other technologies has lead to the new forms of crimes known as “Cyber Crimes”. Cyber crime doesn’t know the physical boundaries and may affect every country in the world.

The transformation in committing crimes with the help of information technology; the law should not be a mute spectator but to transform itself according to the changing environment. There was a need to redefine the old laws in the changing environment. Most of the existing laws in India are either created by the British Government or enacted after the independence within the first three decades and based on physical environment, geographical boundaries, tangible documents and records.

In the digital era, everything is recorded in digits, irrespective of any physical boundaries. Due to these consequences there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. Under these circumstances, E-Commerce Act, 1998 was enacted. After two years of passing of this law, Indian parliament passed “Information Technology Act, 2000” on 17th Oct 2000 to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties & punishments in the field of cyber crimes.\(^5\)

The main purpose of enactment of IT Act 2000 was to reprimand various cyber crimes and to provide strict and harsh punishments. For establishment of Sound Cyber Law Regime various new statute were either enacted or old statute were amended. The

\(^5\) Article Cyber Crimes and the Law
Information Technology Act was amended in the year 2008. In the series of the amendment of old statute, The IT Act amended some of the provisions of. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

With the development of secured electronic transaction technologies more banks have joined the stream to use E-banking both as a transactional as well as an informational medium. As a result, registered Internet banking users can now perform common banking transactions. As the user of E-banking grows and the range of online interaction expands, there is expansion in the cyber crimes. It is evident from the table 1.3 as stated above that cyber crime incidents of fraud in the Commercial Banks in India are enormously increased. **The researcher, in this study has tried to evaluate that how cyber crime affects e-banking in India.**

Though, Information and Technology Act, 2000 is in existence, but with a lot of loopholes. This Act includes law defining and prescribing punishment for cyber- crimes, but this maiden Act has its own limitation. The worst part in IT Act, 2000 with regard to E-Banking is that this act is not applicable to entire Negotiable Instrument Act while the entire banking revolves more or less around negotiable instruments only. The Negotiable Instrument Act was amended in 2002 in respect of cheques in electronic form & truncated cheques; The Information Technology Act 2000 is not encouraging while dealing with the cyber crimes. There are so many discrepancies in the ITAct, 2000 while dealing with the various cyber crimes like copyright, trade mark or patent of electronic information and data. Indian banking industry is facing the problem of growing cyber crime incidents in spite of the Information Technology Act, 2000 & IT Amendment Act, 2008 along with other amended traditional laws like IPC, CrPC, CPC Bankers Book Evidence Act, RBI Act and Indian Evidence Act. to control the cyber crime incidents. **Through this study the researcher has tried to find out the loopholes in the ITAct2000& ITAA2008 and other national laws (old & new) related with banking as to why these legislations are inadequate and insufficient to control the cyber crimes against e-banking.**
The growing reliance on information technology makes critical infrastructure more vulnerable to attacks. This is especially the case with regard to attack against interconnected systems that are linked by computer and communication networks. In those cases, the disruption caused by a network-based attack goes beyond the failure of a single system. Terrorist attack is the unlawful attacks and threats of attacks against computers, networks, and information stored therein. These attacks are done to coerce a government or its people in furtherance of political or social objectives. Terrorist may direct an attack only to disrupt key services. Other terrorist activities like cyber money laundering, terrorism financing and other tools used against banking like hacking, Trojan horse, spreading viruses and worms and denial of services. The Indian Banking Industry is facing the problem of rising trend of cyber terrorism incidents in spite of the enactment of Information Technology Act, 2000 and Information Technology Amendment Act 2008 and also other amended traditional acts to control the various cyber crimes including cyber terrorism. Through this study, the researcher has tried to find out up to what extent the different statute including ITAct, 2000 & ITAA2008 are effective to handle cyber terrorism against e-banking in India.

The most important problem regarding Data Theft in banking is it’s easily access to the computers and computer net work from anytime and anywhere from the world and bears the international nature. The problems are not limited to any statute alone but occur in all the existing statue likes for example, Contract Law, Banking Law, Criminal Law, Evidence Law and Intellectual Property Law. Data Theft is the brain child of Information Technology. The IT Act 2000 not directly deals with the problem of “Data Theft”. The Indian Banking Industry is facing the problem of cyber crime incidents of data theft in spite the different statute are enacted to control cyber crime incidents of “Data Theft”. Through this study, the researcher has tried to find out up to what extent the legal protection under different statute of the land is available for “Data Theft”.


The problem facing by the law enforcement agencies when a citizen of some other country causes harm to citizens of a native country, let's take for an example in India, though Information Technology Act, 2000 does have extra territorial jurisdiction but it is very difficult to enforce it and exercise it. The problems relate to determination of place where the offence was committed and where several jurisdictions are equally competent. 

**Through this study, the researcher has made an attempt to trace out the legal remedies available under cyber law and other laws for extra territorial jurisdiction & extradition of offenders.**

Due to advent of Information Technology, people are using the internet and computers which has linked the people among them irrespective of the caste, creed & religion by demolishing the boundaries of the states & countries. Due to use of internet entire world became a global village. The cyber crime has the global impact and it affects the people of every nook & corner of the world. To face the challenges of cyber crimes, different countries have their domestic laws. **In this study, the researcher has made a sincere effort to compare the existing cyber laws of the various countries to tackle the cyber crime incidents against e-banking.**

There are various challenges of taking legal action against cross border elements and legal question of jurisdiction. There are also the problems relating to the conflicts of law as well as practical issues associated with obtaining evidence, extradition of offenders and international mutual assistance from the countries involved. Without the co-operation of the all countries, single country alone could not be implemented the laws which controls the cyber crime. International organizations, like OECD and G-8 have come forward with a specific plan of mutual co-operation for combating the threat of cyber crime. Barring few countries, majority of them are not responding for their domestic issues. For want of international jurisdictional agreement there is no repatriation of the cyber criminals. Therefore the miscreants can safely operate from these countries and commit the grave cyber crimes. There are problems of prosecuting cross border elements and legal question of jurisdiction and conflicts of law as well as involving practical issues associated with obtaining evidence, extradition of offenders.
and international mutual assistance from the countries involved. **The present study is the effort to evaluate the jurisdictional issues, obtaining evidences from the cross border, extraditions of offenders and international harmonization of the countries involved.**

The expansion of computers has created a number of problems for the law makers of the country and law enforcement agencies. Legislative rules required various records like paper records, signed records, original records and so many other things. The law of evidence customarily depends on paper records and these papers have to be proved in the court though oral deposition and other kinds of physical objects. As more transactions are carried out by electronic means, it becomes pertinent that evidence of these transactions should be available to display the legal rights that flow from and derived from them. The Indian Banking Industry is facing the problems of evidence to prove in the court of law in the digital and electronic form. **The present study is the effort to evaluate the issues of evidence in the digital and electronic forms and attempt to find out the remedy.**

The purpose of the study is to cover the aspects of legal control of cyber crime against e-banking in India. This study is an attempt to evaluate up to what extent, cyber crime affect the e-banking in India. Similarly the researcher has made an attempt through this research work to analyze the effectiveness and efficiency of Information Technology Act, 2000, Information Technology Amendment Act, 2008 and other national laws(old & new) for controlling the recent developments in Cyber Crimes against e-banking in India.

*****
1.3 OBJECTIVES OF THE STUDY

The objectives of this research work are to touch all the important facets of the legal control of cyber crimes against e-banking in India in a comprehensive way and to achieve new insights into it. The main objectives of the present study are as under:

1) To study the progress of the banking in India and implementation of various banking reforms in the banking sector in India.
2) To study the current developments, emerging scenario and building blocks in banking sector in the light of technological advancement in the Indian Banking.
3) To study the meaning and concept of e-banking.
4) To understand the working and authenticity of e-banking in India.
5) To study the meaning & concept of cyber crimes specifically related with e-banking.
6) To study the offenses related with cyber crimes specifically related with e-banking in India.
7) To study the problems of law to control the cyber crimes against e-banking in India.
8) To evaluate the significance of various existing national and international laws related with e-banking in India.
9) To point out the loopholes in the existing national laws to control the cyber crimes against e-banking in India.
10) To compare the existing cyber laws of the various countries for controlling the cyber crimes in the respective countries.
11) To suggest the remedial measures in respect of the legal control of cyber crimes against e-banking in India.

Legal provisions are proving insufficient to control of Cyber Crimes and providing remedies to the customers & banking institution. Moreover, the existing national laws are not sufficient to deal with the domestic e-banking transactions. Therefore this study will throw light on the insufficiency of legal remedy for e-banking and will suggest where the full proof amendments in legal provisions are required to facilitate legal control of cyber crimes against e-banking in India.
1.4 REVIEW OF THE LITERATURE

A number of books, reports, research papers and articles are referred to complete the study with the subject of legal control of cyber crimes against e-banking in India.

A) Books


M.I.Tannan\(^7\) in his book “Banking Law & Practices,” the author gives the every details knowledge about the banking laws & practices in India. It has covered every aspect and every law prevalent for Banking Regulation in India, the book reflects the early history of the banking in India.

Hogson, N. F\(^8\) in his book “Banking through the Ages,” the author describes the early banking system in the various parts of India.

S.B.Verma, S.K.Gupta & M.K.Sharma\(^9\) in their book “E-Banking and Development of Banks” described the general history of banking. The Authors further described the adoption of IT in banking has undergone several changes with the passage of time. Today IT has become an inseparable segment of banking organization. The application of information technology in the banking sector resulted in the development of different

\(^7\) Tannan M.L “Banking Law and Practice in India”, 28\(^{th}\) edition, India Law House Connaught Place, New Delhi.
\(^8\) Hogson, N. F. Banking Through the Ages, (1926) New York, Dodd, Mead & Company
concepts of banking such as – E-banking, Internet Banking, Online Banking, Telephone Banking, Automated teller machine, universal banking and investment banking etc

**Nandan Kamath**\(^{10}\) in his book “Law relating to computers, Internet and E-Commerce (A guide to Cyber Laws and the Information Technology Act, 2000),” the author commented on the cyberspace as it becomes a money spinner and it will increasingly become the domain of business legal & illegal. As a potential information technology power, India should take warning from the hunting hackers and put the legal system on guard. The author also discussed the importance of electronic evidence in the case of cyber crimes. He further added about the legitimacy of the electronic records to be produced as electronic evidence. He exhaustively explained about the burden of proof related to electronic evidence

**R.C.Dutt**\(^{11}\), in his book “Civilization in Ancient India,” the author in his book described in detailed about the banking in ancient India

**Buhler**\(^{12}\), in his book “The laws of Manu, the Sacred Books of the East,” the author in his book discussed in detailed the provisions of punishment as per “Manusmriti”.

**Rupa Mehta and Rohinton Mehta**\(^{13}\) in their book “Credit Cards a Legal Guide” with special reference to Credit Card Frauds, the authors described the proliferation of credit cards in our daily lives and the billion dollars of fraud perpetrated using credits. The authors commented on Money and Plastic Money, Types of Cards, Smart Cards and features of Cards. He explained the Card Cycle. They further discussed Credit Card Fraud and Fraud detection techniques. They explained Credit Card Fraud Investigation techniques. The authors further commented on Credit Cards and Criminal Law and the Liability of Banks & Card holder.

---


\(^{11}\) Dutt R.C., “Civilization in Ancient India” Vol.1, revised edition

\(^{12}\) Buhler, “The laws of Manu, the Sacred Books of the East”, Vol.XXV,p.286

Austin, Granville\textsuperscript{14} in his book "Working a Democratic Constitution – A History of the Indian Experience", described the prevailing economical financial situation before the nationalizations and how Indira Gandhi the then prime minister had taken the decision of nationalization of 14 big banks under the control of private management to boost the perception of social control.

Justice Yatindra Singh\textsuperscript{15} in his book “Cyber Laws” has described the adoption of IT in banking has undergone several changes with the passage of time. The application of information technology in the banking sector resulted in the development of different concepts of banking such as – E-banking, Internet Banking, Online Banking, Telephone Banking, Automated teller machine, universal banking and investment banking etc. Information technology has a lot of influence on banking transactions. He further threw light on trademarks, copyrights, patents & their existence in cyber space.

Toor, N.S\textsuperscript{16}, in his book “Handbook of Banking Information”, the author described that the automation in the banking sector has come a long way starting with the Rangarajan Committee report on the banking sector reforms during the eighties, followed by reports of the Narasimham Committee in the nineties. He threw light on the core banking solutions (CBS, ) RBI guidelines on Universal Banking, Clearing Corporation of India Ltd. (CCIL) and Anti Money Laundering Act, 2002.

Manikyam K.Sita Mrs. Dr. \textsuperscript{17} in her book “Cyber Crimes” Law & policy perspectives described the basic concepts of cyber space like meaning, types, features and major components of computers; history and development of internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. She highlighted the importance of computers and internet in day-to-day jobs. She further expressed that cyber crimes touches and influences almost every aspect of daily routine of each one.

\textsuperscript{14} Granville Austin,”Working a Democratic Constitution – A History of the Indian Experience”. New Delhi: Oxford University Press1999
\textsuperscript{15} Singh Yatindra Justice, Cyber Laws, Universal Law Publishing Co. Pvt. Ltd. 2010
\textsuperscript{16} Toor, N. Handbook of Banking Information,Skylark Publications, 28\textsuperscript{th} edition 2009
\textsuperscript{17} Manikyam K.Sita Mrs.. Cyber Crimes” Law & policy perspectives 2009 edition ,Hind Law House Pune
We are in the information age and dependent on computers as those are the source of inspiration. She threw light on the Information Technology Act 2000 and Information Amendment Act 2008. She also pointed out the loop holes. She also described the comparative study of cyber laws of the different countries.

N. C. Jain\(^\text{18}\) in his book “Cyber Crimes,” the author discussed about the technology based cyber crimes like Viruses and worms. He explained the various varieties of virus like Stealth virus, Polymorphic Virus, Sparse infector a virus that infects the computers only occasionally, Companion virus that creates a new programme by doing modification in an existing files, Armored virus, Macro virus, Virus hoax. He also explained the worms which uses a network to spread functional copies of it to other computer systems. He also described the “Trojan Horse” which is a program that locates password information or makes the system more vulnerable to future entry or may simply destroy programs or data on the hard disk. He also described about Website Compromise and Malware Propagation. He also described the various malwares like Adware, Bots, Bugs, Ransomware, Rootkits and Spyware.

Sinha, S. L. N.\(^\text{19}\) History of the Reserve Bank of India, the author in his book described the history and formation of the Reserve Bank of India

Baibridge D.\(^\text{20}\) in his book “Introduction to Computer Law”, the author described the cyber frauds, its definition and types of the cyber frauds. He also described the ATM frauds and Card Trapping Attack. Skimming Attack, Phishing/Vishing Attack, Pin Cracking Attack, ATM Hacking. ATM Malware Attacks, Carders, the people who buy, sell, and trade online the credit card and Internet Search Engine/Google “Hacking”

Vivek Sood\(^\text{21}\) in his book “Cyber Crimes, Electronic Evidence and Investigation Legal Issues” has described the nature and types of cyber crimes and recommended various

\(^{20}\) Baibridge D., Introduction to Computer Law, 4th Ed. 2000
\(^{21}\) Sood Vivek , Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010
methods to control cyber crimes. He further described the electronics evidence in the
court and its critical analysis and stepwise process; He also explained the electronic
evidence and criminal investigations. He critically analysis the burning problem that why
India should sign the convention on cyber crime and why it is essential He concluded
that cyber and computer related crimes cannot be fought on a standalone basis and
nations must come together to combat these crimes and for collection of electronic
evidence with respect other crimes.

Vivek Sood,²² in his book “Cyber Law Simplified” the author criticized the Power of
Arrest without Warrant under the IT Act, 2000.He threw light on Cyber Crime and
Criminal Justice, He also discussed Penalties, Adjudication and Appeals under the IT
Act 2000. He discussed the Contracts in the Cyber World and Jurisdiction in the Cyber
World. In this book he also discussed Battling Cyber Squatters and Copy right
Protection in the Cyber World. He critically analyzed Digital Signature, Certifying
Authorities and E-Commerce. He further discussed the Indian Evidence Act of 1872 and
Information Technology Act 2000.

Ahemad Farooq Dr²³ in his book “Cyber Law in India”(Law of Internet), the author
described the Development of computers and Internet. He further described the
potential and problems of the Internet. He discussed the Genesis, Objects and Scope of
the IT Act. He threw light on Encryption, Authentication of Electronic Records and
Electronic Governance. He described the Certifying Authorities, Domain Name Disputes
and Trademark Law, Electronic Commerce and service Providers Liability for Copyright
Infringement. He also explains the Cyber Appellate Tribunal. He also described the
classification of Cyber Crimes.

“Harish Chander”²⁴, in his book “Cyber Laws and IT Protection”, the author described
the International Efforts relating to Cyber space Laws and Cyber Crimes. He further
described the council of Europe Convention on Cyber Crime, He commented on the

²³ Ahemad Farooq Dr. in his book “Cyber Law in India”(Law of Internet) published on Pioneer Books Delhi,

Jonathan Rosenoer, in his book “Cyber Law: The Law of the Internet” the author discussed the Copyright and Trade Mark in the Cyber Space. He further discussed the defamation and privacy issues and criminal liability. The author commented on Electronic Contracts and Digital Signature. The author further commented on E-commerce and cyber laws. He further commented on misappropriation of Information and Evidence.

Russell G.Smith, Peter Grabosky and Gergor Urbas, in their books “Cyber Criminals on Trail” the authors defined the cyber crimes and measured the cyber crimes. Further they discussed how the prosecutors are acted as gate keeper of Cyber Crimes. The authors commented on the cross border issues and strategies of Cyber Crime Legislation. They discussed in the book the quest for harmonization of Cyber Crime Law and judicial punishment in cyber space. At the last they described the sentencing Cyber Criminals.

B) Articles

Bhagvati R. Pipaliya in his article “An Empirical study on Consumer Awareness on Internet Banking in Gujarat” discussed the e-banking and the popular services including Automated Teller Machines, Credit Cards, Debit Cards, Smart Cards, Electronic Funds Transfer (EFT) System and Cheque Truncation Payment System and Mobile Banking. He further discussed the advantages of e-banking. The main advantages are the operating cost per unit services is lower for the banks. It offers convenience to customers as they are not required to go to the bank’s premises. There is very low

26 Russell G.Smith, Peter Grabosky and Gergor Urbas, “ Cyber Criminals on Trail” published by Cambridge University Press,2004
incidence of errors. The customer can obtain funds at any time from ATM machines. The credit cards and debit cards enables the Customers to obtain discounts from retail outlets. The customer can easily transfer the funds from one place to another place electronically.

Shamsul Haq and Bilal Mustafa Khan\textsuperscript{28} in their article \textsuperscript{1} “E-Banking Challenges and opportunities in The Indian Banking Sector” commented that banks could be able to reduce the rush at the branches and operating cost also therefore. Banks are now spending heavily on information technology front but from the side of the government there is requirement to invest on the infrastructure like electricity and internet. It is useful from the view of clients as well as the banks therefore in the coming years E-banking reshape the traditional banking.

R. K. Uppal\textsuperscript{29} in his article “Internet banking in India: Emerging risks and new Dimensions” highlighted the benefits of i-banking to customers as well as to bankers and suggests some strategies with their possible solutions like to spread awareness regarding I-banking and to increase its area and scope to enhance I-banking services in India, particularly in rural and semi-urban areas.

Jyotiranjan Hota\textsuperscript{30} in his article “Growth of ATM Industry in India” concluded as Though, ATM industry is growing rapidly, there are many challenges related to security issues of the software, increase of rental costs by the day in major cities, housekeeping, and replenishment of cash. Few banks have introduced biometric ATMs in rural India, which are quite secure and easy to use by a common man. Banks are trying to shift slowly from multi vendor to multi channel integration, so as to get a complete picture of the activities of customers.

\textsuperscript{30} Hota J. “Growth of ATM Industry in India” published in CSI Communications February 2013
Behra, Abhimanyu\textsuperscript{31} in his article “Cyber Crime and Law in India”, has classified the various types of cyber crimes on the basis of nature and purpose of the offence committed. It can be broadly grouped in three categories based on the target of the crimes, a) where computer is the target of crime. b) Where computer facilitate commission of crime. c) Where computer is incidental to the crime and also suggested strategies to control the cyber crime. The major suggestions are a) The Act should be amended suitably in consonance with the development of Science and Technology, b) Cyber cells shall be formed in all the police station throughout the country. Net policing is the need of the hour. c) Judges and police officers and lawyers must be given appropriate training about cyber laws and its enforcement.

Mittal R. K. and Dhingra Sanjay\textsuperscript{32} in their article that transaction through technology channels cost much less to the banks than the customers reaching the bank and doing the transactions. In the last decade banks have invested heavily in the technology. In the use of information technology, the new private and foreign sector banks have taken lead over the public and old private sector banks. Today public sector banks are investing heavily in technology to compete with the new private and foreign sector banks.

Radhakrishna Geeta and Pointon Leo\textsuperscript{33} in their article “Fraud in Internet Banking: A Malaysian Legal Perspective”, commented that the paper examines the legal issues specific to internet banking, focusing on the incidence of fraud and its prosecution. The objective of research is to investigate three questions in relation to Malaysia. Firstly, the incidence of fraud in internet banking; secondly, the adequacy of the relevant regulations and statutes; and thirdly, whether the setting up of a cyber court would better facilitate the prosecution of such financial crimes in Malaysia. Technology and the borderless nature of the internet present fraudsters with manifold opportunities.


‘Phishing’ leads to identity theft and ‘money laundering’ has been found to be the main threat to internet banking, the selected fraud for study in this paper.

Rahul Goel\textsuperscript{34}, in his article “The Indian Information Technology Act and Spamming” pointed out that as per International Telecommunication Union (ITU), "although there is no a single solution to overcoming spam, appropriate legislation and effective enforcement are two of the main elements in the fight to combat the problem. As the phenomenon of spam is relatively recent, not all countries have spam laws, and even those that have already implemented specific legislation are currently facing the problem of enforcement at the national and international level. Furthermore, spammers (often also scammers) are increasingly exploiting the international nature of the Internet. For this reason, cross-border cooperation is crucial both in the elaboration and the implementation of new legislation and in its subsequent enforcement.

Hebbar Raveendranath\textsuperscript{35} in his article “Building trust in E-Banking”, described that Managing Technology is a key challenge for the Indian Banking Sector. Banks have enhanced their network and communication infrastructure to reap the full benefits of computerization. E-banking is catching up. The need for having required tools for trust, privacy and confidentiality is a major area of concern for today’s network banking. Public Key Infrastructure (PKI) provides the frame work of trust essential for e-business to strive. PKI system are used to generate & verify Digital Signature, which can be attached to messages for imparting necessary authenticity integrity and non repudiation policies, procedure and systems are being laid out by RBI and the Structural Financial Messaging Systems (SFMS) being introduced in bank under the aegis of IDBRT is expected to revolutionalize the way banking is conducted in the country. The Real Time Gross settlement (RTGS) system being introduced in the country is built the trust level guaranteed by the SFMS backbone.

\textsuperscript{34} Goel Rahul, “The Indian Information Technology Act and Spamming” Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1 (http://www.arraydev.com/commerce/jibc/)

Shreyan Singh, Sohrab Singh Chhatwal, Taha Mohammed Yahyabhoy and Yeo Chin Heng\textsuperscript{36} in their article “Dynamics of Innovation In E-Banking” concluded as By applying the Revised Technology Life Cycle to two discontinuous e-banking innovations – ATMs and Internet Banking, we have established that the Life Cycle provides a useful outline for successful strategies that can be adopted by banks and other financial institutions as technology evolves.

C) Websites:
The researcher has visited the various websites and goes through the information related to subject. Similarly various e-books were visited on the website and collected the related data for the study. The comprehensive list of the websites is given in the bibliography.

D) Newspapers:
Some national news papers as well as the local newspapers were gone through for the news related to cyber crimes as well as cyber laws. The list of such news papers is given in the bibliography.

E) Magazines:
The various law magazines as well as the other magazines like IBA bulletin, RBI Bulletin and various banks home magazines were read for information related to cyber crime as well as cyber laws. The necessary information was jotted down and used in the study. The list of such magazines is given in the bibliography.

\textsuperscript{36}Shreyan Singh, Sohrab Singh Chhatwal, Taha Mohammed Yahyabhoy and Yeo Chin Heng in their article “Dynamics of Innovation In E-Banking”
1.5 RESEARCH METHODOLOGY

This research is conducted under the supervision of Dr. Alim Khan, Professor School of Studies, Faculty of Law, Pt. Ravishankar Shukla University Raipur (C.G).

As the cyber crimes incidents against e-banking are increasing day by day therefore this study requires examining the impact of legal control of cyber crime against e-banking in India. Cyber laws of the nations are enacted to check and control the cyber crimes incidents against e-banking. If the cyber laws of the country are enough competent and efficient to check and control the cyber crimes then there is no growth/ or controlled growth in the cyber crimes. To examine the growth of the cyber crime incidents and for the purpose of statistical analysis and drawing inferences following data has been chosen.

1) Indian Computer Emergency Response Team – India (CERT-In) is a functional organization of Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. The Information Technology Act, 2000 by virtue of Section 70 A and Section B designated CERT-In to serve as the national agency to perform the functions of collection, analysis and dissemination of information on cyber incidents in the area of cyber security. CERT-In has started publication of data since 2004 on the various cybercrime incidents.

The cyber crime incidents related to banking published by CERT-In taken as under:

1. Phishing,
2. Network Scanning/Probing,
3. Spreading Virus/Malicious Code,
4. Spam,
5. Website Compromise and Malware Propagation and
6. Other Incidents.
7. Total Cyber security

The total of these cyber incidents is also taken into consideration. For the purpose of Statistical Analysis and drawing inferences a period of 9 years has been chosen commencing from 2004 to 2012.
2) Reserve Bank of India published data of Cyber Crime incidents of fraud in Scheduled Commercial Banks in India every year since 2004-05. For the purpose of Statistical Analysis and drawing inferences a period of 9 years has been chosen commencing from 2004-05 to 2012-13.

Data of Cyber Crime fraud Incidents taken from Commercial Banks in India as under:

Table 1.4 List of Scheduled Commercial Banks in India

<table>
<thead>
<tr>
<th>S.N.</th>
<th>PUBLIC SECTOR BANKS</th>
<th>PRIVATE SECTOR BANKS</th>
<th>FOREIGN BANKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(A) NATIONALISED BANKS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Allahabad Bank</td>
<td>Axis Bank Ltd.</td>
<td>American Express Banking Corporation</td>
</tr>
<tr>
<td>2.</td>
<td>Andhra Bank</td>
<td>Development Credit Bank</td>
<td>Barclays Bank PLC</td>
</tr>
<tr>
<td>3.</td>
<td>Bank of Baroda</td>
<td>Dhanlaxmi Bank Ltd.</td>
<td>Citi Bank N.A.</td>
</tr>
<tr>
<td>4.</td>
<td>Bank of India</td>
<td>Federal Bank Limited</td>
<td>Deutsche Bank (Asia)</td>
</tr>
<tr>
<td>5.</td>
<td>Bank of Maharashtra</td>
<td>HDFC Bank Ltd.</td>
<td>Firststrand Bank</td>
</tr>
<tr>
<td>6.</td>
<td>Canara Bank</td>
<td>ICICI Bank Ltd.</td>
<td>Hongkong &amp; Shanghai Banking Corp. Ltd</td>
</tr>
<tr>
<td>7.</td>
<td>Central Bank of India</td>
<td>Bank of Rajasthan Ltd. (Merged With ICICI)</td>
<td>Standard Chartered Bank</td>
</tr>
<tr>
<td>8.</td>
<td>Corporation Bank</td>
<td>IndsInd Bank Ltd.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Dena Bank</td>
<td>Jammu &amp; Kashmir Bank</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>IDBI Bank Limited</td>
<td>Karur Vysya Bank Ltd</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Indian Bank</td>
<td>Kotak Mahindra Bank Ltd.</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Indian Overseas Bank</td>
<td>Laxmi Vilas Bank Ltd</td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Punjab National Bank</td>
<td>Tamilnad Mercantile Bank</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Syndicate Bank</td>
<td>The Royal Bank Of Scotland</td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>UCO Bank</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Union Bank of India</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>United Bank of India</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>Vijaya Bank</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(B) STATE BANK GROUP

| 1.   | State Bank of India |
| 2.   | State Bank of Bikaner &Jaipur |
| 3.   | State Bank of Hyderabad |

(C) STATE BANK CORE GROUP

| 4.   | State Bank of Indore (Merged with SBI) |
| 5.   | State Bank of Mysore |
| 6.   | State Bank of Patiala |
| 7.   | State Bank of Travancore |

(i) PUBLIC SECTOR BANKS=26 (ii)PRIVATE SECTOR BANKS=15 (iii)FOREIGN BANKS=7

TOTAL COMMERCIAL BANKS (i+ii+iii)=48

37 www.rbi.org.in (2013)
3) The Minister of State for Finance, Shri Namo Naraian Meena in a written reply to a question in the Lok Sabha on 22\textsuperscript{nd} February 2013 replied that the details furnished by Reserve Bank of India (RBI) in respect of Scheduled Commercial Banks pertaining to frauds relating to ATMs/Debit Cards/Internet Banking and Credit Cards for the last four calendar years i.e. 2009 to 2012\textsuperscript{38}. We have chosen the data for the Public Sector Banks for the 4 calendar years i.e. from 2009 to 2012 for the purpose of Statistical Analysis and drawing inferences. List of public sector banks is given in the table no1.4

1.5(A) SOURCES OF DATA

The study is entirely based on the secondary data and trust has to be on bona fide published data by the government and government agencies. The Publication of the Reserve Bank of India, Indian Banks Association, Indian Computer Emergency Response Team – India (CERT In), Press Information Bureau of India, Ministry of Finance publications and Government of India publications provide source of trustworthy and authentic data of the secondary nature. A questionary method and primary data source was not selected as the data relating Commercial Banks through published sources is more reliable. As the Bank management would not share the information as it is treated as confidential hence primary source of data collection is not adopted.

Statistical data of Government organizations like Reserve Bank of India (RBI), National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team – India (CERT In) published on their official website has been collected and used in the present study. Similarly, annual publication by RBI on Banking and Finance, Quarterly RBI Bulletins, Publication of Indian Banks Association Chartered Accountants of India and Government of India is also consulted in this study. Data published by the Banks and institutions like the SBI, IDBI, PNB and Nationalized and foreign Banks is also used for this research work.) and published on their official websites as well as in the monthly,

\textsuperscript{38} Press Information Bureau of India Ministry of Finance published the news on 26\textsuperscript{th} February 2013
quarterly and annual publications of the individual banks is also consulted and collected from there for the present study.

As we are considering and analyzing the National as well as International Laws in the light of the E-Banking, the basic data has been drawn from the decided cases from the High Courts and Supreme Court of India. The cases have been drawn from Appeal Cases (AC), All India Reporter (AIR), Supreme Court Cases (SCC). We have consulted Bare Act, books, websites, news papers, case laws, articles and journals for conducting the research. Comparative analysis of cyber laws of various countries has been made in this study for getting an idea of cyber crimes at the international level.

1.5(B) DATA ANALYSIS
The secondary data collected from authentic sources like the RBI, CERTIn and others have been arranged in a series and analyzed the data by using percentage to compare a series of data to describe the relationship among the variables. For statistical analysis of data and testing the hypothesis, “t-test” is used.

1.6 HYPOTHESES OF THE STUDY
[I] The following hypotheses have been set up for testing statistical significance of
1) Cyber Crime incidents of Cyber Securities published by Indian Computer Emergency Response Team – India (CERT In),

   1) Hypothesis-Cyber Crimes Incidents of Total Cyber Security

   **Null Hypothesis H1o:** Existing Cyber legislations are adequate and sufficient to control the cyber crimes incidents of total Cyber Security against e-banking in India; therefore there is no significant growth in the cyber crime incidents of total Cyber Security against e-banking in India.

   **Alternate Hypothesis H1α:** Existing Cyber legislations are inadequate and insufficient to control the cyber crimes incidents of Total Cyber Security against e-banking in India; therefore there is a significant growth in the cyber crime incidents of Total Cyber Security against e-banking in India

2) Hypothesis-Cyber Crime Incidents of Virus & Malicious Code

   **Null Hypothesis H2o:** Existing Cyber legislations are adequate and sufficient to control the Cyber Crime incidents of Virus & Malicious Code against e-banking in India;
therefore there is no significant growth in cyber crime incidents of Virus & Malicious Code against e-banking in India

Alternate Hypothesis H2α: Existing Cyber legislations are inadequate and insufficient to control the Cyber Crimes incidents of Viruses & Malicious Code against e-banking in India and there is a significant growth in cyber crimes in cyber crime incidents of Virus & Malicious Code against e-banking in India.

3) Hypothesis-Cyber Crime Incidents of Website Compromise & Malware Propagation

Null Hypothesis H3o: Existing Cyber legislations are adequate and sufficient to control the Cyber Crime incidents of Website Compromise & Malware Propagation against e-banking in India; therefore there is no significant growth in Cyber Crime incidents of Website Compromise and Malware Propagation per year against e-banking in India

Alternate Hypothesis H3α: Existing Cyber legislations are inadequate and insufficient to control the Cyber Crime incidents of Website Compromise & Malware Propagation against e-banking in India and there is a significant growth in Cyber Crime incidents of Website Compromise & Malware Propagation against e-banking in India

4) Hypothesis-Incidents of Cyber Crime of Phishing

Null Hypothesis H4o: Existing Cyber legislations are adequate and sufficient to control the cyber crimes incidents of Phishing against e-banking in India; therefore there is no significant growth in cyber crime incidents of Phishing per year against e-banking in India

Alternate Hypothesis H4α: Existing Cyber legislations are inadequate and insufficient to control the cyber crime incidents of Phishing against e-banking in India and there is a significant growth in cyber crimes incidents of Phishing per year against e-banking in India

5) Hypothesis-Cyber Crime Incidents of Network Scanning/Probing

Null Hypothesis H5o: Existing Cyber legislations are adequate and sufficient to control the Cyber Crime incidents of Network Scanning/Probing against e-banking in India; therefore there is no significant growth in cyber crime incidents of Network Scanning/Probing per year against e-banking in India
Alternate Hypothesis H5α: Existing Cyber legislations are inadequate and insufficient to control the Cyber Crime incidents of Network Scanning/Probing against e-banking in India and there is significant growth in cyber crime incidents of Network scanning/probing per year against e-banking in India

6) Hypothesis-Cyber Crime Incidents of Spam

Null Hypothesis H6o: Existing Cyber legislations are adequate and sufficient to control the Cyber Crimes incidents of SPAM against e-banking in India; therefore there is no significant growth in cyber crime incidents of Spam per year against e-banking in India

Alternate Hypothesis H6α: Existing Cyber legislations are inadequate and insufficient to control the Cyber Crime incidents of Spam against e-banking in India and there is significant growth in Cyber Crime incidents of Spam against e-banking in India

7) Hypothesis-Cyber Crimes Incidents of Other Offences

Null Hypothesis H7o: Existing Cyber legislations are adequate and sufficient to control the cyber crime incidents of Other Offences against e-banking in India; therefore there is no significant growth in cyber crime incidents of Other Offences against e-banking

Alternate Hypothesis H7α: Existing Cyber legislations are inadequate and insufficient to control the Cyber Crime incidents of Other Offences against e-banking in India and there is a significant growth in cyber crime incidents of Other Offences against e-banking

[Ii] The following hypotheses have been set up for testing statistical significance of Incidents of Cyber Crime of Frauds against e-banking in Commercial Banks in India published by Reserve Bank of India

8) Incidents of Cyber Crime of Frauds in Commercial Banks in India

Null Hypothesis H8o: Existing Cyber legislations are adequate and sufficient to control the incidents of cyber crime of frauds against e-banking in Commercial Banks in India; therefore there is no significant growth in incidents of cyber crime of fraud against e-banking in Commercial Banks in India

Alternate Hypothesis H8α: Existing Cyber legislations are inadequate and insufficient to control the incidents of cyber crimes of frauds against e-banking in Commercial Banks in India and there is a significant growth in incidents of cyber crimes of frauds per year against e-banking in Commercial Banks in India
The following hypotheses have been set up for testing statistical significance of Incidents of Cyber Crime of Frauds against e-banking in Public Sector Banks in India published by Reserve Bank of India in reply to the question in Rajya Sabha

9) Incidents of Cyber Crime of Frauds in Public Sector Banks in India

**Null Hypothesis H\textsubscript{90}:** Existing Cyber legislations are adequate and sufficient to control the cyber crime incidents of frauds against e-banking in Public Sector Banks in India; therefore there is no significant growth in cyber crimes incidents of frauds against e-banking in Public Sector Banks in India

**Alternate Hypothesis H\textsubscript{9a}:** Existing Cyber legislations are inadequate and insufficient to control the cyber crime incidents of frauds against e-banking in Public Sector Banks in India and there is a significant growth in cyber crimes incidents of frauds against e-banking in Public Sector Banks in India

1.7 THE STRUCTURE OF THE STUDY - CHAPTERISATION

The present research work has been divided into five chapters.

1. **Chapter I – ‘Introductory’** includes introduction to the background of the progress of banking industry, government’s initiation of the banking reforms in the banking sector, adoption of banking technology and dawn of e-banking in India. The chapter also describes the research problem of the study in the area of cyber crimes & e-banking in India. The chapter simultaneously describes the objectives of this study to touch all the important facets of the research. The chapter furthermore describes the methodology employed and gives an overview of literature. This chapter describes the sources of data and data analysis. This chapter framed the hypothesis

2. **Chapter II – Progress of banking in India, meaning & concept of e-banking, meaning & concept of cyber crimes in banking and cyber crimes offenses related with banking.** This chapter describes the progress of banking and the various phases of the banking. This chapter discusses the meaning & concept of e-banking and its progress in India. It also depicts various e-banking products & services provided by Indian banking industry. This chapter simultaneously discusses the meaning & concept of cyber crimes and offenses related with cyber crimes in banking sectors. This chapter
also throws light on the factors responsible for rising of cyber crimes in the banking industry in India

3. Chapter III – Legal problems to control cyber crimes against e-banking in India.
This chapter describes the financial sector reforms since 1991 in the banking sector and government provided the necessary platform for the banking sector to operate on the basis of operational flexibility and functional autonomy; enhancing productivity, efficiency and profitability. This chapter further discusses the existing legal frame work in India. This chapter looks at problems of law to control cybercrimes against e-banking in India. This chapter describes an exhaustive study about the existing legal provisions in India and how these legislations are efficient to enforce them to control the mounting cases of cyber crime against e-banking. This chapter describes the critical evaluations of IT Act, 2000 and IT Amendment Act 2008 including other existing laws (old & new) related to e-banking. This chapter simultaneously describes grey area of these legislations. This chapter further discusses the problem of mounting incidents of Cyber Crime in India and the issues of data theft, cyber terrorism, cyber jurisdiction in cyber space and extradition of offender and problems of evidence in cyber crime cases.

4. Chapter IV – Comparative Study of Laws of different countries regarding Legal Control Of Cyber Crimes. This chapter critically examines the comparative study of national & internationals laws on legal control of cyber crimes against e-banking. This chapter throws light on issues relating to domestic & international laws relating to jurisdiction in the cyber space. This chapter also discusses the need for international cooperation to combat cyber crimes. It takes into account various Conferences, Conventions, Summits, and Treaties on the subject of cyber crimes and cyber laws

5. Chapter V – Observation and discussions, Suggestions and Conclusion. This chapter addresses the observations on the overall research work. This chapter further discusses the testing of hypothesis. This chapter also discusses final outcome of the analysis of the data. This chapter throws light on the grey areas of Indian cyber laws. This chapter addresses the conclusions and suggestions arrived at as a result of the discussions in the previous chapters. In this chapter the shortcomings and lacunae in the cyber laws are pointed remedial measures suggested to ensure effective legal control of the cyber crimes against e-banking in India.