CHAPTER 2

REVIEW OF LITERATURE

(**Brar and Singh, 2012**) As per the survey conducted 70% of the respondents replied that they are not using the internet banking when the reason was asked for non use they replied that they are reluctant to use internet banking as they feel it is unsafe to use and they have a fear of becoming the victims of e-banking frauds. It shows that there is a major security issue and legal issues. Customers do not have confidence in using internet banking services. Therefore the research conducted clearly states that the customer still do not want use the e-banking services and according to them there is chance of losing their money if the fraud is committed. According to the customers there is a high possibility of them facing the problems and issues of e-banking frauds if they start using or are using the e-banking services provided by their respective banks?

(**Chavda, 2014**) the research states that one of the reason for increase in e-banking frauds is, as amongst people in India there is lack of computer literacy so they not know how to use the e-banking services and if they want to use, then they have to take help of someone which will lead to customer disclosing his secret data and which can be misused by fraudsters. The Knowledge about using the computer is must if the person wants to use the e-banking services otherwise the risk of e-banking frauds goes high.

(**Chakrabarty, 2013**) According to the survey conducted by Reserve Bank of India around 1,76,547 banking fraud cases were reported and the amount involved was Rs 31401.01 crores out of which 1,69,190 cases were reported in the commercial banks and amount involved was Rs 29910.12 crores. Public sector Banks reported 29,653 cases, 93,331 cases were reported in Private sector Banks and 46,206 cases were reported in Foreign Banks. 65% of fraud cases were committed because of technology related issues such as internet banking frauds, credit card frauds, and other e-banking frauds.
(Chavan, 2013) has stated that the meaning of electronic banking is providing banking services and products to the customers through electronic delivery channel such as internet banking, mobile banking ATM facilities and Credit cards etc. This article has explained about the variety of channels used for the doing of the banking transactions and taking the advantage of the advancement of the technology to the fullest of the extent.

(Doiphode, 2014) article states that in order to have safe and secured e-banking the bank staff handling and controlling e-banking system must be adequately trained and properly selected. Thus it is always advisable to select the person who is honest and dedicated to his work for the various posts in the e-banking system operating, controlling and handling department. Most of times the fraud is committed by the fraudster easily because the staff looking after the e-banking system is not that capable enough to handle the look after the system either not qualifies or not that much experiences to handle the system. The recruitment at this post needs the prime importance as the money will be lost of the individual if the person so appointed does not do his job properly of handling the electronic banking system.

(Hussain and Srivastava, 2014) article states that there were about 26,402 case reported of phishing in 2011. Deceptive phishing, malware base phishing, session hijacking, data theft and Domain Name System based phishing etc these kinds of phishing attacks are practiced on customers by fraudsters and they are successful in doing so because of lack of education and knowledge to customers and technology issues. Solution to it is installation of anti phishing techniques and by educating customers through awareness campaigns and advertisements that they should not click on hyperlinks provided in emails. This is the most common type of fraud which is taking place and easy to commit as people get attracted by the emails of getting prizes or winning prizes and then they land us giving out their bank details.

(Singh, 2012) has defined online banking as system which allows customers to use banking services from a personal computer by connecting with the banks computer over the telephone wires. E-banking benefits the banks by reducing their cost and also catching up the customers from the remotest areas. E-banking is benefited to the customers also as 2X 7 banking services are available to them, banking services are
provided to the customers at their home or offices some other benefits are electronic transfer of funds, online bill payments, anytime cash withdrawals from ATMs, Credit card facilities, customers can access the accounts online through internet banking etc. Even the merchant and traders are benefited avoids all the problems involved in handling the cash, increase in business due to increase in purchasing power of the credit cardholders, trading at international level can be done easily. Due to e-banking there is globalization of trade and establishment of e-commerce which will lead to development and overall growth of the nation. 59% of the respondents were unaware about the e banking. Therefore this article is highly related to the e-banking services provided by the banks across the globe.

(Jagtap, 2014) a survey conducted amongst the educated respondents shows that 38% of the customers are still non user of online banking because of low security level, risk of fraud and no guidance for operation. It is concluded that inspite of being educated customers are reluctant to use online banking as they feel it is unsafe to use. The improper knowledge, training and guidance to the banking personnel’s, results in to the increase in the number of e-banking fraud cases. No timely upgradation of technology and maintenance of security standards are also the reasons of commission of e-banking frauds are the large scale.

(Jamwal and Padha, 2009) article states that, Reserve Bank of India had formed a working group to find out the challenges faced in internet banking. The group found that the major issues are relating to technology and security issues, legal issue and regulatory and supervisor issue. One the bases of the report prepared and submitted by working group to Reserve Bank of India (RBI), RBI prepared the various guidelines to be followed by banks. Banks have stated implementing but somehow they are not adequate enough in controlling and preventing e-banking frauds the ineffectiveness of RBI guidelines can be also because of customer’s behavior. Thus inspite of guidelines provided to take safety and security measures and banks implementing the same yet the cases of e-banking frauds are on increase every year. The article makes us know what all efforts the government has taken to reduce the cases of e-banking frauds.
(Jassal and Sehgal, 2013) the research have stated that although few banks have framed security policies but they are proved to be ineffective because there are various loopholes and mistakes or they are incomplete, or inefficient, in most of the banks security polices for users does not contain the tips for the users about do’s and don’ts, security policies for banks are ambiguous and they do not explain clearly privacy statements to the customers, there is inadequate policies even for user Ids and passwords, network providing hardware & software systems are also not properly designed and upgraded regularly, back up policies are also not framed in proper manner.

(Jha et al, 2014) the article states that phone phishing is one of mode of identity theft; identity theft means stealing someone personal details to have access to their confidential financial data and that will be misused by fraudsters to commit the frauds. The confidential information’s are received by the fraudster through use of the phone as stating I am calling from XYZ Company and you have won the price so we need your bank account details such fake calls are made to the customer and information’s relating to customers account are taken from them which are then misused. Identity theft is one of the easiest methods of committing the fraud in the area of e-banking as the entire concept of e-banking services is based on the data that is the details of the person.

(Jokhi, 2014) article states that Mr. Milind Deora, the ex minister of State for Communication and Information Technology, had said that the total loss suffered because of e-banking frauds by Indians as per Reserve Bank of India report was around Rs.54 crores in first half year of 2013-14. E-banking frauds are increasing each year out of which some cases are reported and others go unreported in India due to lack of cyber law awareness in India.

(Karimzadeh and Alam, 2012) article states that the major obstacles in development of electronic banking are legal issues, security issues and technical issues due to which e-banking frauds are committed in order to prevent the same and have development of e-banking there is a need for proper implementation of legislations, security policies to be adapted in order to build up confidence in the minds of customers that, e-banking services are safe and secured to use, awareness to be done
on preventive measures to be taken by customers to avoid the incidence of e-banking
frauds. Making people aware about such measures would prove a best remedy to the
problem and the safety environment can be created for the using of e-banking
services.

*(Khanna and Arora, 2009)* research states that lack of training and low compliance
level of Reserve Bank of India guidelines are the main reasons of e-banking frauds.
They have suggested that a regular internal control on e-banking system one of the
preventive measure for which quality training is needed to be provided to the banks
staff, the people who are handling and have internal control over electronic banking
system because generally fraudsters tries to identify loopholes in the control
procedures. The guidelines given by the RBI are not followed to the fullest of it extent
this is a reason the number of cases relating to e-banking fraud case are increasing
each day.

*(Komal and Rani, 2012)* the study states that there are majorly four channels e-
banking ATM, credit cards, internet and mobile banking. 29% of respondents feel that
mobile banking is not reliable and 24% of respondents feel that use of credit cards is
not safe. Mobile banking is highly risky as the people have the habit of downloading
the applications which are free and through these free applications fraudsters remove
the detail data from the mobile of the person stored in it and also they keep a constant
eye on the messages which are received by the individual which would give them the
information’s useful in committing the e-banking frauds.

*(Kundu and Rao, 2014)* E-banking frauds are safe crime does not harm or cause any
injury to the body of the fraudster. It is difficult to find the fraudsters of e-banking
crimes and even the investigators are finding it difficult to locate the fraudsters.
Survey states that around 455 fraud cases were reported during 01.01.2007 to
30.09.2010 which includes credit card frauds, ATM frauds, staff frauds etc. The few
of suggestions made to prevent e-banking frauds are effective security policy to be
framed by banks, regularly monitor internal management, to provide training to the
staff handling e-banking system, regular upgradation of technology and banks to have
compulsory in house grievance settlement body, more and more investigating cells to
be established and appointment of efficient investigators to be made.
the study defines the various types of e-banking frauds like Hacking means unauthorized access to data stored in computer system. Phishing means receiving of e-mails by customers from fake sites looking same as the original website of financial bank send by fraudsters requesting customers to click on the link and enter their user name, password or any other personal information’s in order to have access to their accounts for any particular reason. The data received by the fraudsters will be used by him to commit the frauds. The websites created by the fraudsters are so identical that it is very difficult for an individual to recognize the same as the normal man of prudence would be capable of recognizing the same.

according to the survey done around 2760 fraud cases were reported relating to technological issues which are nearly about 65% of the total number of fraud cases. It is observed that security issues are also faced by customers due to loopholes in technology which leads to data stealing and data is misused by fraudsters making the customers suffer huge losses. Therefore technology is needed to be up graded on regular basis. This article has focused on the issues relating to technology and commission of the e-banking frauds which has to be maintained as per the guidelines given by the RBI. RBI guidelines are must to be followed by all the banks in India.

article states that G. Gopalkrishna committee set up by RBI in 2011 recommended certain suggestions out of which one of it states that fraud review council must be formed in all banks by the fraud risk management group to review frauds and take preventive steps regularly, but yet the suggestion given has not been implemented by all the banks providing electronic banking services to their customers.

study states that there are various types of internet banking risk one of it is information security risk, lack of data relating to personal detail security techniques exposes banks data and customers details to hackers or insider attackers by inserting viruses and stealing the data and the same is used by the fraudsters in committing frauds, therefore causing financial losses to the institutions.
There are various frauds committed in the e-banking sector relating to Automatic Teller Machine, credit card frauds such as phishing attacks, identity theft; data stealing, hacking, cracking, malware attacks and many more this is leading to huge financial losses to the country at large. This article states about the tools used for doing transactions through e-banking services and also regarding the certain types of e-banking frauds.

The research states that if you want to prevent phishing attacks then anti-virus and spam filter software’s are to be installed, even firewalls should be kept on. Customers should access the website only through internet browser status bar or through typing the word “https://” at the start of the URL address in the address bar.

Research states that 64.83% respondents have agreed that mobile banking is not secured while downloading certain applications customers give way to fraudsters to access their data stored on mobiles easily for example through their messages, gallery and various files and folders containing confidential data so there is threat of data theft that might cause the customers to be the victim of e-banking frauds.

Research states that computer is taken as tool for committing the frauds as computer is having huge data stored including secret data and information’s also, computer is easily approachable to steal data by secretly implanted key loggers and logic bombs. The data obtained is misused and after using it is destroyed so the proof of facts and evidences are also lost sometimes if there is no proper backup. Mobile is also used as a tool for committing frauds.

The research tells us that people are not aware about the e-banking frauds like Phishing out of 50 respondents only 16 were aware, spoofing only 12 respondents were aware etc. Some preventive measures are to be taken by the customers for reducing these e-banking frauds like not to forget the ATM card anywhere, not to disclose the Personal Identification Number to anyone, never give the credit card information when it is asked on phone, not to reply phishing emails, to always use the websites that are secured. Internet and Mobile Association of India
(IAMAI) found that around 43% of customers are not doing transactions on banks websites in India because of security issues.

(Singh, 2012) the article states that various kinds phishing techniques practiced by the fraudsters. The various cases were reported by ICICI Bank and later on even by United Trust of India bank and State Bank of India and others. In India there are several cases relating to attacks on genuine websites.

(Singhal and Padmanabhan, 2008) a research states that out of 61 respondents only 35 % respondents agree that internet banking is reliable which shows that there is lack of confidence amongst the customers due to security issues. During the use of online banking customers have become the victims of phishing attacks, identity theft and data stealing which were used by fraudsters in committing fraud. The electronic fraud can be committed by fraudsters either because of negligence of customers or else negligence on the part of the banks.

(Soni and Soni, 2013) research states that the Gopalakrishna Working Group (GGWG) has give various mandated recommendation on preventive measures to be taken by banks in order to have safe and secured e-banking services such as each bank providing electronic banking facilities have to create a separate information security body, which will exclusively look after the management of protecting the information’s and will also frame security policy and get it approved from board and policy to be at least reviewed annually but all the banks in India have not implement the same till today.

(Usman et al, 2013) article states that challenges faced with the technological development in the banking sector are security issues and legal issues. Most of e-banking cases are reported due to weak internal control systems and phishing. More than 35.9% of the banking sector is the target for phishing, ATM frauds, credit card frauds, stealing of funds, stealing of data over the years there has been increase of about approximately 12% in identity theft victims. There is urgent need to take preventive measures in order to prevent e-banking frauds.
The research states about the assurance and responsiveness of public sector and private sector banks towards customers who have been victim of the e-banking fraud. E-banking system is always under threat from malware attacks by hackers. A study states there are security issues which leads to data stealing and business users are victims on regular bases. There are also legal issues for which amendments are needed to be made in rules and regulations relating to e-banking frauds. If the security system it not updated properly and regularly it will lead to cracking and hacking of the system using lacuna in security system. Out of 100 respondents 25% of customers agree that they cannot rely on the bank for not misusing their data available with them and do not trust on security system of banks. Existing systems are reliable but not 100%. 32% of respondents do not agree that information technology units provide them sufficient support. A survey concludes that e-banking services are not widely adopted by the customers. E-banking services means people understand only online balance enquiry and online bill payment there are not aware about digital checks and online check book reconciliation. 42 % of the customers are not satisfied with various e-banking services provided by their respective banks. Therefore this article majorly tells us regarding the hacking which is now a day’s become very common issue while using e-banking services. There is an urgent need to create awareness about e-banking services by arranging seminars and conferences. 27 % of the customers are not satisfied with the ATM services provided by the banks. A large number of customers are dissatisfied with web links. There is a need to design the web page with due care by using latest technologies. There is a need to educate the employees in order to increase their ability for handling customer’s problems.

The study analysis the success of Information System in internet banking and its security challenges. 52 respondents were surveyed customers have fear that information sent by them through internet is not protected also have threat of their banks website getting hacked. The customers also have the fear of the malware attacks. The customers have the doubt about the security system of being reliable for internet banking services.

55.34 % of the respondents stated that they had moderate knowledge about the internet banking and many of them have just
started using internet banking services. Due to lack of knowledge about using internet banking services there is less level of usage and satisfaction amongst the customers. The banks need to educate their customers regarding internet banking services and increase the confidence level of the customers by convincing them the e-banking system is reliable and well secured

(Shukla and Shukla, 2011) article states that the customers using electronic banking services do not have trust regarding safety of transaction through e-banking and they also do not trust that their personal data would be confidential and not leaked. The acceptance can be given by banks for opening of the bank account on internet but account to be opened only after following the know your customer norms which states about face to face verification of the detail documents of customers and their identity. The banks in their policies should clearly mention about the stop payment instructions to the customers. At the initial stage only the banks that have physical existence in India was permitted to offer various products through internet banking to people who are residence of India. The banks were given permission to offer products through internet banking only to the account holders. The Upgradation of technology is to be done regularly. The confidential data is just secured by the user name and password which is not adequate enough to keep and maintain confidentiality due to which hackers can get the customers information easily that is biggest threat to the customers using online banking services. It is stated that e-banking have lot of benefits yet it has brought lot of challenges along with it.

(Perumal, 2006) This article states about the security measures for maintaining the confidentiality of the customer’s information. These security measures are helpful in reducing the risk of electronic banking frauds. The current scenario about authentication is done through password which is not adequate enough to maintain the level of security for the customer’s confidential information’s. There is a need to have more efficient security measures in order to protect the customers from being the victim of electronic banking frauds. A biometric authentication is a solution to it, as this is one of the best ways of having security highly maintained. Biometric can be in physical or behavioral say for example finger print, thumb impression, retinal scan, handwriting, voice etc. The study states that finger prints and retina scan are high accurate and reliable. Voice, Iris scan and signature are medium accurate. With the
use of biometric instead of password as a security measure and for authentication 
would be highly reliable and will maintain the confidentiality of the customer’s 
information and will ultimately help in reducing electronic banking frauds. This 
system of biometric is helpful to a great extend if implemented properly although it 
would cost more to the banks for implementing and installing the same at the initial 
age and later on maintaining the same would increase the expenses of the banks and 
also the work of the bank would increase at the back hand.

(Safeena et al, 2010) article states that that there has been transformation of manual 
banking transactions to electronic banking transactions through various channels such 
as automatic teller machine, debit card, credit cards, internet banking etc. The study 
states about the customers perspective towards internet banking. The customers are 
not ready to adopt the electronic banking system due to fear of hacking, data stealing 
and they are also worried about the protection of their personal information. For 
making the customers adopt internet banking banks have to educate the customers as 
to how to use the internet banking services and make them aware about the various 
benefits and uses of e-banking services. Banks also need to make aware to the 
customers regarding the risk factors involved while using e-banking services and 
educate the customers regarding the preventive measures to be taken by them while 
using e-banking services.

(Gupta, 2006) There are laws framed in India under Information technology Act, 
2000 for the protection of the data such as section 66 states about the hacking as an 
offence. Although there are laws in India enacted for the purpose of data security they 
are not adequate enough even the Information Technology Act has lacuna as the act 
only states about the offences which are committed by one who breach data security 
procedures the act does not state about the obligation on the organization to 
implement the data security measures compared to under United Kingdom laws banks 
are under obligation to maintain security measures in respect of data as per Data 
Protection Act, 1998.In India if the transaction are done through internet then the 
banks are not liable it will be the internet service providers who will be liable for data 
theft. India laws relating to data protection are needed to be amended to bring in par 
with other nations laws.
This article states about the domain name system. Domain name system has unique names and has a lot of data saved. The data in the main zone is also available in 13 computers around the world. The IP address of the main server is known to all the other resolvers. Resolvers do contact any one of the servers for information about high level domains. As the servers are crucial to successful domain name resolution so they have been regularly subject to attack called as distributed denial of service attack. Fraudsters take control of various machines on the internet and send a flood of queries to main servers to overwhelm them. So while designing the Domain name system one need to be very careful.

The electronic banking in Ethiopia is still not developed because of the few challenges faced as due lack of infrastructure that is internet facility, there are no suitable laws to regulate the electronic banking services. There are no laws framed and enacted to deal with enforceability and validity of e-commerce contract which includes banking services. There is no high rate of literacy due to which people don’t know how to use the electronic banking services, the cost of internet is also high, there is frequent power off, there is also fear of risk involved amongst the people while using electronic banking services as there is lack of security. Ethiopia needs to enact the rules and regulations to govern the electronic banking system. As in Information Technology Act is for frauds committed relating to e-banking and the offence is committed in country like Ethiopia where there are no laws only of such kind then because of the question of jurisdiction of case the accuse will be set free and victim will get no justice.

Article states the various challenges faced with the development of technology in the banking sector. Majorly there are security issues. There is lack of confidentiality and threat of data stealing amongst the customers. There are number of legal issues also faced. There is lack of customer trust on e-banking. There is lack of awareness amongst the customers relating to e-banking as how to use such technology and how to prevent frauds by taking preventive measures. There is lot of risk involved relating to leakage of personal information’s while using electronic banking services. If all these problems are solved then the electronic banking has a lot of benefits.
(Kesharwani and Gajulapally, 2013) this article states about specifically hacking and fraud risk and many other risk involved while using internet banking services. The study states that in 2009 only 12% of the online users were preferring internet banking services to do the transactions. Study states people do not feel secure for conducting bank transactions through internet banking system, they feel it is unsafe as web sites may be misused or hacked by fraudsters. The information on bank website relating to e-banking is not clear and understandable. There is possibility of data stealing and personal information while using internet banking, the internet connectivity may also be lost while using internet banking which would leave the transaction incomplete and it would be risky. Mainly the customers have fear of security issues and legal issues and they feel internet banking is unsafe and not reliable.

(Singh, 2011) The study states that majority of the customers have stated that mobile banking is not good. People choose the bank on the bases of level of security and convince. Due to fear of security risk involved and legal risk the customers are not willing to change and adopt the electronic banking system. There is also lack of awareness amongst the customers at the same time.

(Goel, 2006) The article mainly states about the phishing, spamming and latest amendments made in Information Technology Act, 2000. The IT Act, 2000 did not prove effective in reducing the crimes relating to electronic banking. There are number of cases relating to data stealing and misusing the same. In order to bring amendment in the existing legislation an expert committee was appointed by the government of India to look into the privacy and protection of confidential data and give their recommendation and suggestions on the same. Committee gave various recommendations relating to privacy issues but kept silent on the issues such as phishing and spamming. Section 66 of Information Technology Act does not cover the acts relating to misrepresentation on internet through which user is compelled voluntarily to give his personal information, such acts are called as phishing. The fraudsters host a website with same domain name which looks like original regular banks website. The customers think that he is logging on the banks website and gives the information asked for which is used by fraudsters to commit the frauds. The legislation needs amendment and to include many new offences relating to electronic
banking in simple and understandable way without ambiguity so the fraudsters can be punished and victims can justice.

*(Dash et al, 2014)* Article studies about the mobile banking, it states that mobile network service providers to assure the security to their customers especially when customers are doing banking transactions. In 2008 Reserve Bank of India has given guidelines on mobile banking which are to be followed by all the banks that are providing mobile banking services. Study states that customers are not adopting mobile banking as they have no or less knowledge about how to use as many of the customers are not techno savvy, customers don’t find mobile banking safe and secured. Few customers that have adopted mobile banking are facing the problems of frauds being committed due to lack of knowledge and awareness about what precautions customers need to take when they are using mobile banking services.

*(Kumar and Ravindran, 2012)* a study states that the respondents feel that using mobile banking will allow unauthorized person to have access to their personal information and that would be harmful as this personal and financial information’s can be misused by the fraudsters. Respondents also stated the mobile banking has increased the chances of data theft and frauds. There is lack of knowledge amongst the customers for using mobile banking which could involve lot of risk of data leakage as survey states that mobile banking users should be experts otherwise committing mistakes would lead to data theft and ultimately data will be misused for committing various financial frauds. As mobile banking is done through public channel that are open, so there are high risk of data theft and security risk. In this case as per Reserve bank of India guidelines for mobile banking banks have to maintain high standard security level to keep the confidentiality of private data of their customers. It is very truly and correctly said that the mobile banking involves the lot off risk.

*(Velmurugan and Velmurugan, 2014)* article states that there is neither much knowledge and nor much awareness which is one of the reason people are not using mobile banking. There are number new model being designed, customers do not know how to operate and there are lot of application which customers are not able to understand how to use. So due lack of knowledge about using mobile banking
applications there is risk of data theft and data leakage which can lead data access to unauthorized third person and this data in turn will be misused to commit financial frauds and other frauds.

(Singh, 2014) study states that there less than 1% people who are using mobile banking although more than half the population is using mobile phones. The reason for customers not adopting mobile as a channel for doing banking transactions is security concern. It is stated that know your customer norms must also be applied to mobile payments. Reserve banking of India has already issued regulations for mobile banking in 2012 as per the regulation given by reserve bank of India the messages on mobile relating to transaction to be generated and delivered to the customers in 10 seconds but that is not so in practical many a time there is delay in receiving messages on mobile relating to transaction. People are worried about the safety and security of their personal information while using mobile banking services; there is also fear of disconnection while doing transactions due to battery low or any other reason. These are above give few of the reasons for which people are still reluctant to use mobile as a channel for doing banking transactions.

(Sharma, 2012) Study states that rural customers are not satisfied with regulatory mechanism and the amount of compensation given to the victim of e-banking fraud committed by the unauthorized person. Respondents also stated that there needs a improvement in the e-banking services provided by the banks. About 72% of the respondents do not feel comfortable in doing banking transaction through e-banking services as their main problem is of language, many of them are also unaware of multi language provision in e-banking system. Respondents do not feel e-banking is safe and secured in order to win the confidence of the customers the banks need to change the password pattern from PIN number to biometric and voice call system for doing transaction through e-banking channels such as ATM, internet etc. Awareness is needed to be created amongst the customer’s by educating them regarding phishing and other types of frauds committed by fraudsters through advertisement campaign.

(Dixit and Datta, 2010) this article states that the security and data confidentiality privacy are the major issues faced by the customers and so they are reluctant to use the e-banking services. Compared to other countries like Australia, Malaysia,
Singapore and Saudi Arabia not much work is done in India on issues relating to e-banking frauds. The study states the various factors due to which adult customers are not accepting e-banking. Out of 200 respondents 24 respondents were just the beginners of learning computer and 21 respondents do not know how to use the computers. 66 respondents have stated that they prefer performing banking transactions through visit to bank instead of ATM, telephone and online banking. Respondents have stated that online banking is not trustworthy. To encourage the adult customers to use e-banking banks need to conduct seminars to educate the customers about uses of e-banking and about preventive measures to be taken by them when they are using e-banking for performing the banking transactions.

(Amtul, 2011) This article states that there are majorly security and privacy issues in using e-banking services that can be solved to some extend by biometric based authentication. Study states that Citibank was the first victim of the fraud committed by the hackers through interfering with the money transfer system which caused loss about 10 million dollars illegally transferred. Legal authorities are always focusing on protection against threat to the security and privacy issues. In few countries special acts are enacted for such kind of issues say for example In Ireland Electronic Commerce Act was enacted, in United Kingdom, United States of America, Australia, New Zealand and Singapore electronic transfer act was enacted, in Honkong and Pakistan there is Electronic Transactions Ordinance and in India there is Information Technology Act. Still the number of losses and fraud cases are increasing for which introducing biometric authentication would be helpful in solving the problem of security threat. Personal Identification Number to be replaced and converted by introducing biometric system. Biometrics means measurable behavioral and physiological characteristics which can be captured and afterwards compared with another instance when verification is done. Through this system financial losses can be prevented. Still the countries outside India have good security system compared to India. As India is still at the developing stage and other countries most named above are almost developed countries.

(Fozia, 2013) Study states that private banks customers are more satisfied as compared to public sector banks customer in regards to e-banking services. Different age group customers have different perception. Mostly the old age group people are
not willing to change and adopt the e-banking. Customers are mainly worried about the security and safety issues therefore banks need to educated customers about the safety measures that customers have to take say for example customers should not disclosed their PIN number to anyone and should also not store in the mobile where anyone else can access and misuse it for the fraudulent purpose. Customers need to change their PIN number regularly these preventive measures if taken would help in eradicating the chances of e-banking frauds.

(Redwanuzzaman and Islam, 2013) There are lots of benefits of e-banking services. Along with the benefits there are many challenges also faced. The major challenge faced were relating to regulatory issue, security issue and other management problems. These challenges need to be resolved in order to induce more and more people to use e-banking services which will ultimately help in growth of the nation.

(Sabi, 2014) Article states that internet banking is still not adopted completely in the developing countries such as South America, Caribbean and many African areas due to problems that are involved in using internet banking. People in developing countries do not want to change from manually transacting banking transactions to internet banking as they are having fear about security, safety, trust and privacy issues about 56.9% respondents have stated so, 18% respondents have stated that there is lack of computer literacy and knowledge about internet amongst the customers, 7% respondents have stated that there is lack of awareness about internet banking, more than 7% respondents have stated that bank web sites are not properly designed these all should be solved and the same is already mentioned in the laws to improve the internet banking but the implementation of the same is lacking which creates the problem and gives a way to increase in number of internet banking frauds and less people adopting internet banking. Therefore in order to induce more and more people to use internet banking the above given problems are needed to be resolved.

(Paschaloudis and Tsourela, 2014) this article studies about the quality of the bank websites providing internet banking services, the customers using electronic banking services through bank website is done through E-S _ Qual and e- RecS - Qual scales. Due to the bank website not properly designed and of poor quality there is lot of challenges faced, as to mention few people do have security issues and privacy issues
which ultimately results in financial frauds being committed while conducting banking transactions through these bank websites. The banks are also not responsive in handling the problems pertaining to e-banking frauds. Compensation given to the victims of e-banking fraud is also not adequate enough. The quality of bank website is needed to be maintained by the banks and high level of security is to be maintained by the banks.

(Shannak, 2013) This study states that the legal and regulatory coverage in Jordan are still unsatisfactory. Customers still do not have trust on e-banking. It is stated that e-banking based transactions are easily copied, saved and stored and are highly insecure compared to paper based transactions also there are number of intermediate parties such as internet service providers, telecommunication carriers etc, involved in e-banking based transactions so chances of data leakage is also high and they can also easily copy, store the transactions while passing it from one computer to another through network. Because of these reasons legal issue while using e-banking is challenging. One of the challenges is as if the fraud is committed who would be held responsible the bank, customer or the internet service provider or telecommunication service providers. The study states that there is also the risk of phishing involved. The laws need to be amended as there is lot of ambiguity involved which will ultimately help in reducing e-banking frauds and win the customers trust. This question of responsibility of frauds will always remain the question as it would depend on the facts and circumstances of the case which would be different in different cases.

(Khan and Khan, 2012) this article states that the customers attitude towards internet and mobile banking. As in the recent trend after internet banking came the mobile banking. Most of the banks and the financial institutions have started providing mobile banking services which the customers find more ease and gives rapid information’s and transactions can be done more faster. In the study it was found that few customers is preferring internet banking and few customers are preferring mobile banking as while using internet banking the person has to sit in front of the computer for a longer period of time and the same is not in the case of mobile banking. Mobile banking services can be used by customers at any time and any place as each one now a days have the mobile phones in hand. Few of the customers are reluctant to use both internet banking and mobile banking as they few it is not secures and there are
privacy issue, legal issues and technology issues. So finally it was concluded while doing the comparison between internet banking and mobile banking that the services provided to the customers and usefulness of both are same but still mobile banking and internet banking are different from each other.

(Munusamy el at, 2012) the study states regarding the challenges or obstacles faced while adopting internet banking by the Malaysian retail banking customers. The various obstacles faced are such as customers were finding it difficult to operate or they are hastate to operate may be due to lack of education and knowledge even if they know how to operate the computers they were making mistakes of clicking the wrong button which would cause a great loss to the customers, sometimes the connectivity is loss in between while doing the transaction of internet which would again cause risk of loss to the customers, the customers are worried about the security issues and they feel that internet banking is not safe and secured, customers feel that internet banking is not reliable and lot of risk is involved, Customers are reluctant to use internet banking as time for completing the transaction is very less and many a times the transactions do not get completed in the time provided are half left which would be risky. Customers have no trust in internet banking. There for it is said that level of obstacles or challenges faced are increasing with customers adopting internet banking services which need to be faced and controlled through imposing legal provisions o control and prevent the same. The technology is needed to be up graded regularly by the banks.

(Amin, 2010) The research states that the ATM is useful for making deposits, cash withdrawals also for balance queries. The study states that inspite of having so many benefits customers are not using e-banking services. Tabung Haji is one of the Islamic financial institution in Malaysia, where the customers were refusing to use the ATM services provided by the banks. Mainly ATM banking was started for two reasons, firstly it provides the customers flexibility, convenience and cost saving option for doing their banking transactions. Secondly by introducing ATM Facility 24 hours banking service was offered to the customers. Customers were reluctant to use ATM banking services initially as it was new technology with which they were not familiar. Later on survey conducted of 140 respondent’s states that customers were worried about the privacy and security issues while using ATM banking services for doing
their transactions. So countries still do not have a full proof security system there are still loopholes in the same which needs to be removed in order to have safe and secured e-banking facilities for the customers.

(Alam et al, 2010) study states that the technological development has made possible financial transactions in banking industry globally. Online banking has given lot of benefits to the customers. Research states that this online banking facility has not yet been provided to the customers in all the places all over the world there are still few places where this online banking facility is not available to the customer’s one of such place is Sudan. As there are number of challenges faced in implementing the online banking system to name them 77 % respondents strongly agree that there is lack of infrastructure to support the service, there also lack of technological skills but still they tried to implement it. 80 % agree that there were security issues faced to protect the data leakage by the hackers, large number of population was uneducated so they could not use internet banking therefore 56% respondent strongly agree that the customers did not know how to use internet banking so they were reluctant to use the online banking services, 62 % of respondents strongly agree that bank employees handling online banking system were properly trained which would lead to high factor of security risk to the customers, there was frequent network breaking down which would again be risky. Research states that only 20% of respondents were fully aware about online banking system.

(Altintas and Gursakal, 2007) the research states that because of data theft, privacy issues due to theft of customers personal identity data, security issues due to phishing attacks and internet frauds customers do not trust and lack confidence in the internet banking system. The survey conducted states that majorly there is security related risky involved while using internet banking system, as the number of cases related to phishing attacks and internet banking frauds are increasing every day. The reason for increase in number of internet banking frauds is lack of knowledge and education amongst the customers regarding internet banking system. Most of the customers are reluctant to use the internet banking services for doing banking transactions due to the security risk involved as the system is not safe and secured so lot of data theft, personal identity theft and internet banking frauds are taking place. Due to security
issues lot of customers are facing various problems while using internet banking services.

(Zhengchuan and Zhang, 2012) this article states that Phishing has become one of common way of electronic banking frauds. There is a threat of security as the personal information’s are steeled by the hackers very easily through phishing attacks. Phishing attack means it is a trick played to compel the person to give away this personal information’s which misused for committing the frauds. Phishing attacks are increasing at faster rate in the present scenario and ultimately leading to the security issues while using online banking services. There is about 81% increasing in Phishing attacks since first half of 2006. Research states that more than 1, 57,000 phishing messages are sent to various people in the year of 2006. The financial losses caused to the customers due to phishing attacks is approximately in billions of dollars it is difficult to accurately measure the financial losses caused to the business organizations and individual customers. Hence because of increase in number of phishing attacks huge number of customers are become victims and are suffering huge financial losses, therefore customers are reluctant to use electronic banking services and the one who are using electronic banking have the continues security threat.

(Omar et al, 2011) the study states that online banking has benefited to the customers in many ways by saving their time and all time banking transactions are possible simultaneously there are drawbacks of using internet banking services which are there are security issues, there is lack of trust on internet banking services amongst the customers and even there is lack of knowledge as to how the internet banking is to be use because of this reason there reason many internet banking frauds committed . This study helps the banks to improve the services of online Banking services. Safety and security are the foremost important challenges faced while implementing the internet banking services and the same are the difficulties faced by the customers who are already using internet banking facilities. Out of total 37 respondents, 15 that is majority of them were not satisfied with the security system of internet banking services especially of automatic teller machines, out of 37 respondents 11 of them said that they were not satisfied with the internet banking services provided by the banks. The banks need to improve the security system in order to win the trust of their customers.
(Fahim, 2012) this article states the amount of risk involved in using internet banking services. The amount of trust customers have on internet banking services and the awareness amongst the customers regarding internet banking services. Most of the respondents did not have the knowledge as to how to use the internet banking services and many of the respondents do not want to use the internet banking services as there is lot of security risk involved according to them in using internet banking services. These are the few factors affecting the implementation of the internet banking service.

(Suki, 2012) the study states that the factors influencing customer satisfaction and trust on mobile internet banking. Research states that few of the customers do not have trust on the mobile internet and therefore they do not use the mobile banking services. The quality of website is also that good and the service providers do not have safe and secured network as there are frequent cases of data theft due to which there are number of mobile internet banking fraud cases reported every day.

(Yuan et al, 2010) this article states about the internet banking in china. Internet banking system was first started in china in the year 1997. Till 2002 more than 3.5 million customers had opened Internet banking accounts. With the rapid growth in use of internet banking system for banking transactions the security risk and other threats such as data theft, number of banking frauds also started rising. Internet banking system is most of adopted by the young, highly educated and wealthy people others still continue with manual way of doing banking transactions. Most of people in china are not aware about the use of internet banking services its benefits and there is also lack of computer literacy amongst the people. Internet banking system is of lot of advantage to customers as it is cost saving also yes large amount of customers are still not using internet banking services because of the problems such as lack of knowledge, awareness, education and security related issues.

(Zimucha et al, 2012) The transformation of banking sector from manual transaction to electronic transaction because of technology development has give rise to various issues such as security issues, data theft, frauds, criminal activities and other threats and risk. The study states that the customers’ accounts are being hacked and tampered through phishing or identity theft. A survey was conducted to know that banks use
how many security strategies and it was found that most of banks are using maximum four to five electronic banking security strategies. Commonly used strategies are firewalls, encryption, personal identification number and passwords. Zimbabwean commercial banks have still not started using virtual keyboards for an e-banking security strategy only 19.4% of the commercial banks have implemented virtual keyboards as a security strategy. Personal identification number strategy is widely implemented by the banks. 60% of the respondents have stated that the security strategies presently implemented are effective but not to full extend. 40% of the respondents have stated that the resent security strategies implemented are not effective. It is suggested that the biometric security strategies should be implemented by the Zimbabwean commercial to have a safe and secure e-banking services to be offered to the customers and win the trust of the customers

(Olatokun and Bankole, 2011) this article states that one of the challenges faced in implementing e-banking technology is security issues, although e-banking has lot of benefits still there are lot of issues in using such an advanced technology. One of the other issues is there is lack of technology qualified staff to look after the e-banking service provider system because of which there are high chances of e-banking frauds. There are high chances of theft as the security equipment to protect the data from getting leaked for example personal information’s, credit card and bank account related information’s and so on are not adequate enough. Therefore the customers are still reluctant to use the electronic banking services. These issues need to be resolved in order to make more and more customers use electronic banking services.

(Adewole, 2015) This article states about the confidence level amongst the customers regarding payment system. As the consumer payment is the main responsibility of banking companies. And the most recently used mode of payment is through electronic transfer of fund and online banking payment, use of debit card and so on. The research states that only about 11% of the respondents are using electronic transfer of fund as a way for banking payment which means customer do not have confidence in the system and majorly they prefer to do the transactions manually through cheque based system of payment. Around 62% of the consumer does not have the confidence in electronic mode of payment system. 94.3% of the consumer lack confidence due to frauds prevailing while using the system, 77.2% lack confidence
due to poor consumer protection, 88.1% agrees that consumer is exposed to lot of risk. Only 32.7% respondents rated for the online banking system of payment through ATM, credit card, and debit card and so 93.8% of the respondents have stated that confidence level in e-banking payment system is less due to security and safety issues. This problem needs to be resolved in the developing countries in order to win the confidence of the customers in the electronic banking payment system.

(Rathore. D, 2015) Cyber crime is also called as digital wrong. An illegal committed through the use of computer as a tool. Cyber crime has affected many sectors and one of them is banking sector which majorly affected causing huge financial losses to the customers. Different types of cyber crimes committed by fraudsters in banking sector are identity or data theft, phishing, ATM frauds and so on. Through technological development banking sector has started providing banking services to their customers through electronic medium which has benefited to their customers but along with this development in the banking sector any challenges were faced as many frauds are committed by hacking the banks websites and it results into theft of money causing to customers huge financial losses. Another one is credit card frauds which is also very famous. Next is email frauds through phishing which means sending fake emails in order to reveal personal information’s of the customers which the fraudsters use later to commit the banking frauds. Therefore it is rightly said that banks need to pay first attention on the security system in order to protect the confidential data of their customers from getting leaked and being misused by the customers.

(Jamaluddin, 2013) the article states that the top most ten banks providing electronic banking facilities in India are Citi Bank, Union Bank of India, Canara Bank, Bank of Baroda, Punjab National Bank, Bank of India, HDFC Bank, Axis Bank, ICICI Bank and State Bank of India. Study states that only around 7% of the account holders in India are using internet banking for doing the banking transactions. Electronic banking has benefited to the customers at large scale at the same time there is a negative effect of the electronic banking as this has given rise to various issues such as identity theft, phishing attacks because of which the customers still do not use electronic banking facilities very few customers have accepted have started using electronic banking services to do the banking transactions. There is a need to study the laws properly and have knowledge about the laws in India and across border
regarding electronic banking system which would help in reducing the electronic banking frauds to some extent and would also help in preventing the incidents of electronic banking frauds.

*(Singh et al, 2011)* that the study states the major issue in implementing electronic banking system in India was the security issues he needed the immediate attention another issue was relating to low computer related knowledge and literacy. There is even lack of awareness amongst the customers regarding the technology use. The legal issues are still prevailing as there is lack of implementation of the Information Technology Act 2000. With the development of technology in the banking sector the latest and safest type of crime was relating to computer system through network. To name few of the frauds are ATM related frauds, data theft and stealing of customers personal information’s by way of phishing, Skimming and spoofing, credit card frauds are the next. Survey conducted states that only 16 respondents were aware about phishing, 12 were aware about spoofing and 32 were aware about spamming out of 50 respondents.

*(Fernandes, 2013)* the article states that with increase in number of customers using electronic payment system, there is tremendous increase in the number of electronic frauds also causing huge financial losses to the customers. The various types of electronic frauds are broadly classified into two online frauds and offline frauds. Online frauds are relating to data and personal information stealing through internet by way of phishing, spoofing and many more. Offline frauds include credit card frauds, debit card frauds, ATM frauds and many more. There is a need to take various steps in order to prevent the electronic banking frauds as soon as possible majorly by implementing the good security measures which would solve the problem to a greater extent of electronic banking frauds. Awareness and education about the preventive measures to be taken and about various types of electronic banking frauds also by reducing risk factors are few of the other ways of solving the issues relating to the electronic banking frauds.

*(Bansal and Suman, 2014)* this article states that there has been increase in number of users using online banking and with it the number of banking fraud cases are also increased causing huge financial losses to the customers therefore there is a need for
immediate action and to keep an watch on the fraudsters. This article mainly focuses on the detection of credit card frauds with the new idea of self organizing maps. The existing legislations and data protection policies are not efficient enough to deal with the problem of online banking frauds. Self organizing maps help in detecting transactions which are hidden and cannot be seen in the usual course. This method of detecting frauds will protect the customers and banks from the fraudsters.

(Nasir et’al, 2015) this article states that the main concern of the customers using Internet banking services is relating to security related risk, privacy risk and financial risk, because of this, there is no positive impact of customers attitude, towards Internet banking services provided by banks in the city of UK. According to the survey conducted there are numerous incidents of frauds by hacking, phishing and so on receiving confidential information of the customers which is later on misused by the fraudsters resulting into great financial losses to the customers? The most customers out of 191 respondents is concerning about the security risk in adopting the internet banking services and hence they have the negative attitude towards internet banking. The security standards have to be raise through legal provisions then can only the attitude of the customers can be converted positive towards use of internet banking services.

(Owolabi, 2010) This article states that there are number of banking frauds practiced out of which one that is recently added is computer frauds as the manual banking system is converted to electronic banking system. Computer is use as main tool or instrument to commit the banking frauds. Most common types of electronic banking frauds are skimming, ATM frauds, debit/credit card frauds, frauds though sending false emails, electronic money transfer frauds and so on. Robberies, forgery and credit card frauds are few of the other common types of banking frauds. This article have stated four theories of banking frauds which are differential opportunity, theory of concealment, theory of deviation and theory of minimal and general collusion. The survey conducted shows that there were around 3087 cases reported of banking frauds in three years from 2003 to 2005. The data states that the number of cases relating to banking frauds is on increase every year. The survey also states that there is much involvement of the bank staff in committing the banking frauds. There is an urgent
need to frame and implement some strict legal provisions against banking fraudsters in order to stop and prevent the commission of the banking frauds in Nigeria.

*(Perkins et al., 2013)* the main issue relating to online banking of the Ghanaian customers is security and safety issue that includes protection of personal identification number, of confidential data from the hackers who misuse the data for the purpose of committing banking frauds resulting into huge financial losses to the customers. Customers do not have trust on the online banking system. The survey conducted states that there were around 3,655 cases reported of phishing which is on increase every day. Ghana government has passed various bills to protect the banking frauds but still the number of cases is on rise. Hence therefore the bank managers must pay attention on the security standards in order to provide the protection to the customers and offer safe and secured online banking services to their customers which can be done by having adequate legislations in order to have the proper implementation of the government suggestions made and then can only banks shall be able to win the customers trust.

*(Bahl, 2012)* the article states that e-banking has many befits but along with it has got various challenges. The major challenges faced by the banks are regulatory issues and supervisory issues. Regulatory and supervisory related issues are mostly relating to the banking transactions cross border. There are also legal challenges faced as the banks can expand the area for providing electronic banking facility and it may be possible that local laws would be applicable only to particular jurisdiction and beyond that jurisdiction local laws would not be applicable which would create a great problems for regulating and supervising electronic banking services as there may be no license required in that area as per the law to provide the customers electronic banking services to their customers. As the laws would be different in that area so the banks would unknowingly break the laws relating to protection of customers data and violate protection and privacy laws and such crimes will not be prosecuted also and no law suits can be filled against such wrongs as it is the crime here but it may not be so in the other areas. The other is security issues which also one of the major challenges faced by the banks. There is a problem of personal data getting leaked resulting into commission of banking frauds. Therefore while implementing electronic
banking system there are many risk involved leading to banking frauds along with the various benefits.

(Jawahar, 2014) the article states that are lot of security related threats which includes unauthorized access to the customers data, confidential information, account by way of hacking or through virus attacks. This unauthorized access to information leads to data theft which is misused by the fraudsters for committing the banking frauds. Hence banks need to have security polices to be framed very carefully. The information technology act 2000 was framed and established to have safe and secured electronic banking services but still the number of cases relating to electronic banking frauds are on rise each day. Either the act is not adequate enough or else the laws are not properly implemented by the banks resulting into huge financial losses to their customers. There is need to have regular changes to be made in the act as the technology is developing very fast so the fraudsters find the way faster to commit the frauds even in the full proof security standards maintained by banks therefore there is a need to keep a regular check on security standards by the banks and make necessary changes same is with the laws necessary amendments are to be made timely when required so to implement the laws effectively.

(Oko and Oruh, 2012) this article states that the security system of the ATM is improved by using fingerprints of the customers as their password instead of personal identification number. This has ensured the customers greater security. The various types of frauds such has ATM card stealing, stealing of personal identification number, skimming, data theft, etc are all related to ATM card frauds. With the use of biometric system for the purpose of password has helped to reduce these kinds of frauds to the great extent. Using biometric passwords such as finger prints, eye retina scanning etc are very much benefited to reduce the electronic banking frauds. Therefore there is need to have all banks providing electronic banking services to their customers to issue biometric system of password compulsorily to safe and secured use of electronic banking services.

(Shanab and Matalqa, 2015) this article states that e- banking has lot of benefits but still it is not fully trustworthy as there are number security issues and other challenges faced relating to e-banking frauds. Mainly the banking frauds are relating
to cross border banking transactions. There are various challenges faced with the emerging trend of electronic banking system to mention few which are most common are regulatory issues, legal issues, security issues etc. There are frauds committed by the skilled professional hackers they manipulate with the banking system containing the customer’s data and is misused to commit the banking frauds. The various types of frauds are phishing, credit card frauds and so on. The proper detention and prevention measures have to be implemented in order to reduce the number of electronic banking frauds.

(Wang and Huang, 2011) this article states that the negative effect of development in the area of information technology is that, it has increased the number of criminals and the cases of crime related to internet commonly known as cyber crimes. Identity theft is one of such crime which is discussed in detail in this article. Identity theft is committed by way of phishing, spyware, hacking, skimming and so on. Skimming is done when the transactions are done by way of swiping the debit or credit. By way of phishing method the fraudsters receive the customer’s personal and financial details in order to commit the banking frauds by stealing the data and then later on misusing the data or information obtained by the fraudsters. Phishing is done via sending emails. Computer is used and is an important tool or devices to commit the frauds or crime of data stealing.

(Yousafzai et al, 2009) This article states that the survey was conducted amongst the 441 customers using internet banking and it was found that still the customers do not have trust on internet banking as there are lot of security issues and privacy related issues are still not resolved. Trust is an important factor involved to translate the banking system fully to electronic form. Therefore it needs an immediate attention and needs to be resolved as early as possible then can only customers can take complete benefit of the technological development.

(Singh, 2008) This article states about the security issues faced while using internet banking services in Australia. Banks have stated that the problems relating to security issues leading to credit cards frauds and have made the customers and merchants responsible for the same. As the banks all the time is giving warning to their customers to be careful especially with their confidential data such as password and
so on. Issues of privacy in the banking sector is of prime concern as there is risk involved of financial losses via fraudulent use of the credit cards by the fraudsters via data theft. Therefore customers do not have the trust on the electronic banking services provided by the Australian banks to their customers.

*(Chiezey and Onu, 2013)* This article states that the fraud and fraudulent activities plays an important role in creating the problem in the electronic banking sector in Nigeria. This has caused the huge financial losses to the customers and ultimately results into economical instability in the country. The Article states that the internal control system is weak and also the regulatory and supervisory system is not adequate enough to keep a check and control on internet banking fraud activities. The information technology system is also outdated which needed to be upgraded regularly in order to control the fraudulent activities.

*(Anwer et al, 2009)* This article states that with the increase in number of customers using credit cards to banking transactions, the number of fraudulent acts have also increased simultaneously in the developing countries. This article has suggested credit card fraud system and prevention technique for the developing countries. Address verification system is one of the techniques which are commonly used in order to prevent the credit card frauds. The various types of frauds include identity theft, skimming, phishing and so on. This technique of Address verification system helps to find out whether the credit is lost/ stolen or not as to what is reported by the cardholder, also check the validity of the credit card, verifies the security code, checks the expiry date and so on therefore as this system is having lot of advantages hence it is very useful to keep a check on the credit card frauds and helps in prevention of credit card frauds.

*(Chauhan, 2015)* this article states that now a days the crimes are committed in area of banking sector with the help of using the technology. Everyday there is an increase in number of bank frauds causing huge losses to the customers. Computer is used a tool to commit the banking frauds. One of the commonly committed banking frauds is relating to ATM debit/credit card frauds and internet banking frauds. The study states that there were about 8322 electronic banking frauds cases reported in 2012. The reasons behind this are that the customers do not have adequate knowledge regarding
the information technology and also the laws relating to banking are in adequate. There is need to have adequate laws in order to control and prevent the electronic banking frauds and reduce the financial losses caused due to such crimes committed in the banking sector.

(Hossain and Hossain, 2012) This article states about the various electronic banking offences. It is stated that because of these offences the customers do not have trust in the e-banking system and are not ready to use the e-banking services. To name few of the e-banking offences are password fraud, debit/credit card frauds, data theft and so on. There are legislations framed on the e-banking frauds in Bangladesh as such there are punishments for the offence of hacking or having unauthorized access to others account, for cracking, for destruction and so on. But still the number of cases relating to electronic banking frauds is increasing everyday in Bangladesh; this clearly states that the laws established in Bangladesh relating to electronic banking frauds are still not adequate enough to prevent the offences of e-banking or else the existing laws are not implemented properly or else the investigation skills are lacking in the officials. There is uttermost need to look into these problems relating to electronic banking offences urgently and have solutions to it in order to avoid any further financial losses that would be committed.

(Ahmad and Al-Zubi, 2011) this article states that the customers are still not sure that the electronic banking is safe and secures hence they do not trust the online banking services. Therefore the bank customers in Jordanian are still not completely satisfied with the internet banking services because of security and privacy issues. There are number of banking frauds committed due to data theft, hacking, phishing and so on.

(Brar et al, 2015) This article states about the threats involved while using the online banking. The survey states that most of the online banking frauds are committed because of the customer’s failure to protect their confidential information such as password and so on. There is continuous increase in number of e-banking frauds every year due to security issues, privacy issues, legal issues and so on In the survey it was found that the customers are still not aware how reliable their banks have the security system neither they are aware that their banks are upgrading the security systems or on, customers lack confidence in security system of their banks. The
survey conducted brings about the result that majority of the e-banking fraud cases which are reported are related to public sector banks as compared to private sector banks.

(Verma, 2015) this article states that the internet banking has been helpful and benefited to the customers at the same there are many issues relating to internet banking such as security issues, identity theft which results into huge financial losses to the customers and this internet banking frauds are committed because of inadequate service provided by the banks to some extent. There is continuous increase in number of phishing attacks, Trojan attacks faced by the customers. There are also legal issues faced as the banks have yet not completely implemented the guidelines issued by the Reserve Bank of India. Amongst all the various kinds of attacks phishing attack are most common and more beneficial to the fraudsters.

(Okibo and Wario, 2014) This article states about the various obstacles in technological development in the banking sector. The various barriers are lack of education, Knowledge, technological know-how, not trust worthy as there is lack of security because of this reasons customers have still not accepted the e-banking system in Kenya. The survey conducted states that out of 135 respondent’s majority of the respondents agree that e-banking is less reliable. 65% of the respondents agree that there are many legal issues and security issues. 45% respondents agree that there are chances of high frauds, 40 % respondents state that there is lack of security of information, 30% respondents agree that there are chances of data lose. In Kenya also there exists the same problem of security issues which the people are facing while using e-banking services.

(Radhakrishna, 2009) this article states that there is lot of security, regulatory and legal concerns relating to e-banking services in Malaysia. There is high risk of financial losses. The various e-banking frauds in Malaysia are phishing via fake e-mails getting the confidential information of the customers and the same are misused by the fraudsters resulting into huge financial losses to the Malaysian customers using internet banking services. There is increase in number of e-banking fraud cases each year.
(Hoseinpour et al., 2015) this article states that survey conducted results into the customers of Keshavarzi bank in city of Kermanshah do not have trust fully on electronic banking and hence they are reluctant to accept the electronic banking services. As there are lot of issues involved in using the e-banking services therefore the customers also think ten times before using the same as one mistake would land them cost a lot so the customers prefer to void such kind of situation to come so they show unwillingness to use the e-banking services and stick to their manual way of doing the banking transactions.

(Dubey and Manna) this article states about the various types of e-banking frauds taking place they are card skimming, spyware, ATM skimming, hacking, identity theft and so on. This article also states about the management to prevent the e-banking frauds such as banks to keep a check on fraudulent activities and trace the fraudsters, awareness to be created amongst the employees and also training is needed to be provided to them as to how to prevent the e-banking frauds and maintain security and confidentiality of the customer’s data.

(Sathyanarayana, 2014) this article states about the challenges faced by customer while using e-banking services as per survey conducted are 22 respondents state that there are weakness in designing the banks website, 16 respondents state that there is lack of awareness regarding technology and 14 respondents state that to some extent there is negligence on the part of the customers. 21 respondents state that there are legal issues.

(Desai and Buch, 2015) this article states about the online banking issues mainly about hacking, theft, identity theft and so on they are all said as crimes. There are some examples given one of the example states that in the email it is showing customer have not correctly entered his internet banking details email says the customer to validate his details one has to click on the link given in the email and link is of the fake website requesting to feed the details of credit card and other personal information this is how data theft is done and is misused by the fraudsters.

(Emenike, 2015) The author in this article states that Nigerian banks have pointed out the legal issues in payment system services. ATM have made the cash withdrawal
facility easy for the customers at a same time there are many frauds committed relating to ATM, smart cards, credit cards and debit cards. Survey indicated that there is about 98% increase in banking frauds in last ten years causing huge financial losses. The customers at Nigeria are facing the problem in using the ATM service and they feel that the use of ATM machine system for cash withdrawal is not safe and secured. The reason being the data theft at Nigeria is to the lager extent, so the number of e-banking frauds is increasing as with the help of data they can easily make the duplicate card and start using the same or with the help of the data they can apply for the new card and the new PIN number. The reason being these issues and fact of not being system safe and secured people do not want to use e-banking services. 

(Pink and Darun, 2014) author in this article states that there are risk involved in using internet banking services. Customers are suffered by criminal attacks and financial losses and hence they do not trust the internet banking system. Criminals may be internal that is the employees handling the e-banking system or the externals they are the hackers and fraudsters. There is security risk involved from internals as well as externals. The appointment of the staff handling the system is of the prime importance for any bank to provide safe and secured e-banking services to their customers and also winning their trust on the bank.

(Makarevic et al, 2014) article states that there are privacy issues relating to customers personal information. After survey being done it was concluded that the customers have negative mind set regarding online banking services as they feel there are high chances or possibilities of financial/ monetary loses while doing the banking transactions online. Another problem is education customer do not have knowledge about online banking services as to how to use. Therefore the customers feel that online banking is not secured and they are prone to high risk from data theft and so on. If the viruses enter while doing the transaction or connection of internet is lost when only half the transaction is completed there may be possibility of data getting leaked. So the customers need to compulsorily install the anti-virus in order to avoid such things to happen. The Anti-virus installed need to be one which is registered and not the one which is unregistered. Although the one which is registered is costly the registered one should be installed because if the fraud is committed that loss would be
definitely more than the cost of installing registered Anti-virus software in the computer used to do the e-banking transactions.

*(C, 2012)* research states the RBI has directed the banks to take insurance considering e-banking frauds were committed due operational risks, but banks did not follow the direction given, they tried to save their cost considering that customers will not raise voice against insecure banking service provided to them. Around 3,700 cases of frauds were reported in Public Sector Banks and 15,700 fraud cases were reported in Private Sector Banks. This shows that banks are enjoying and earning more profits at the cost of customers.