2. REVIEW OF LITERATURE:

(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.

(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.

(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 29653 cases, 93331 cases were reported in Private sector Banks and 46206 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.

(Raghavan and Parthiban, 2014) There are various frauds committed in 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.
A survey conducted amongst the educated respondents shows that 38% of the customers are still non-users of online banking because of low security level, risk of fraud and no guidance for operation. It is concluded that, despite being educated, customers are reluctant to use online banking as they feel it is unsafe to use.

One of the reasons for the increase in e-banking frauds is that, amongst people in India, there is a lack of computer literacy so they do 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.

There are majorly four channels of 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 the use of credit cards is not safe.

Computer is taken as a 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.

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 e.g. their messages, gallery, and various files and folders containing confidential data so there is the threat of data theft that might cause the customers to be the victim of e-banking frauds.

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.

(Muthukumaran, 2008) has defined 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 other personal information to access their accounts for some reason. The data received by the fraudsters will be used by him to commit the frauds.

(Hussain and Srivastava, 2014) have stated 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 education customers through awareness campaigns and advertisements that they should not click on hyperlinks provided in emails.

(Richard and Hintau, 2012) In order to prevent the phishing attacks anti-virus and spam filter software’s are to be installed, firewalls should be on. Customers should access the website only through Internet browser’s status bar or the “https://” at the start of the URL in the address bar.

(Jha et al, 2014) Phone phishing is one of mode of identity theft; identity theft means stealing someone identity to have access to their confidential financial data which is misused by fraudsters to commit the frauds.

(Patil, 2012) have said that here are various types of Internet banking risk one of it is information security risk, lack of data security techniques exposes banks data to hackers or insider attackers by inserting viruses and stealing the data which will be misused by the fraudsters in committing frauds, therefore causing financial losses to the institutions.
People are not aware about the e-banking frauds like Phishing out of 50 respondents 16 were aware, spoofing only 12 were aware etc. Some preventive measures to be taken by the customers for reducing these e-banking frauds like not to forget the ATM card anywhere, not to disclose the PIN 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 43% of customers are not doing transactions on banks internet sites in India because of security issues.

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 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.

The then Minister of State for Communication and IT, Mr. Milind Deora has stated that the total loss suffered in first six months of 2013-14 by Indians as per RBI report was around RS. 54 crores. 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.

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.3700 cases of frauds were reported in Public Sector Banks and 15700 fraud cases were reported in Private Sector Banks. This shows that banks are enjoying and earning more profits at the cost of customers.

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. Customers do not have confidence in using internet banking services.
(Karimzadeh and Alam, 2012) have said 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 proper implementation e legislations are to be made, security policies to be adapted to build up the confidence in the minds of customers that e-banking is 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.

(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. Around 455 fraud case 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 security policy to be framed by banks, monitor internal management, 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.

(Khanna and Arora, 2009) indicated 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.

(Jamwal and Padha, 2009) 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 are reluctant to implement the
same because there is no monitoring committee set up to keep a check, so inspite of guidelines provided to take safety and security measures yet the cases of e banking frauds are on increase every year.

(Soni and Soni, 2013) The various mandated recommendation on preventive measures were give by Gopalakrishna Working Group (GGWG) on safe and secured e-banking services such as each bank to create a separate information security body that will exclusively work for information security management, to frame security policy and get it approved from board and policy to be atleast reviewed annually but banks did not implement the same.

(Parameshwara, 2013) G. Gopalkirshna 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.

(Pasricha and Mehrotra, 2014) 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.

(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 UTI bank and state bank of India and others. In India there are several cases relating to attacks on genuine websites.

(Doiphode, 2014) 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.

(Jassal and Sehgal, 2013) Even if few banks have framed security policies 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.