Review of Literature:

The findings and truth in any literature of searching field gives the basic idea to which our research development scope of the research can be found and laid upon. It is the hard work of the researcher to find and develop the basic ideas of the knowledge obtained by the literature review. There is the need of strict care and full awareness for the sound work to save the research from already done work so that it may not be an empty effort. It should lead some scope for further research.

Inventions or new research are the further stage in any field of finding the truth and original and true ways of search. The researcher should be careful and ready for the new assignment and apply all knowledge which already exist for finding the new one like an empty vassal to be filled with content of new search fields of its scope or marked area. Collecting of new field information and searching the facts of already done work pave the way for further knowledge. Review spontaneously the literature for finding the facts and research in that field give further stages of success. A building foundation of literature review set the goal of the researcher on the right track.

The review of literature gives the clean picture of the problem to be solved as being a prerequisite to actual planning and conducting the study. The researcher be fully prepared for his field or domain and apply the knowledge which he already has got in the field.

One such preparation of gathering the knowledge much has already been done in that area. The truth and findings put the researcher in his domain by analysis of the data and review. So to avoid any unnecessary odd situation in research the literature review is very essential.

Roy Anindya & Chopra Anil (2005)[1] has revealed that hackers are getting new and some surprising techniques to acquire the information of our bank account. The latest ways like phishing and others may lead us to some websites which do not exist there.

Bajaj, K Kamlesh, And Nag, Debjani (2002) [2] - According to it the business done on Internet rely on giving safely and in secured way the information access to companies, collaboration
partners and the customers with full authorization. There are many factors associated with the e-Business security and challenges which need the full proof association of policies with technologies in secured manner. While we implement the standards and policies to the systems which already linked to the business should maintain the security and reliability to the customer about the product.

Internet Security is the basic core of problem in the commercial application. The studies elaborate about the commerce applications success story is inappropriate due to the electronic safety controlling measurements. Establishment of a standardized quantification of security is a manner for ensuring the faith of clients in business on internet usages. Designing and analyzing the e-Business applications give the safety, reliability and security quantifier.

Safety threats in E-business are getting largest concerns from architects and legal bodies. As any change starts from writing on files to Internet and all exchanges take place from large distances of not known places, assuring the originality of business processes and exchanges is very hard.

Security is not a product, nor is IT technology. Security is a process. The process of security consists of many things. It contains preventive control measures and a healthy dose of awareness. It includes disaster recovery and business continuity. Various products and technologies support all of these elements of the process. The process of the security is a state of mind that must permeate a co-operation and its culture to be effective. The hacker can sit and wait and increase the probability of detection, change strategies. A hacker targets products of the huge customer base and each successful attack leads to a very high level of damage and provides wide publicity.

Traditionally, when talking about data security usually four security objectives are identified: confidentiality, integrity, authenticity, audit ability and availability. The most important one is accountability. Below are the security goals to be achieved-

Stop unwanted damage.
Stop the accidental losses.

Control the deletions impacts

Stop the locations unauthorized access.

Ensure the system confidentiality & data integrity.

System disaster recovery should be maintained.

It is very important to create a list of the company’s priorities for a security system. The security with cost reduction in very simple way should be given the important priority for the successful e-Business. User-based security and traffic-based security is a good solution when used in collaboration with integrity for network control measures. According to it steps to be implemented for E-Business Security are given below-

Creating the Security Strategy.

Cryptographic Tools.

Cyber terrorism.

Defenses from Viruses.

Firewall Systems.

Thus following these upper said directions then we can form safe and secure the entire e-business network.

De Tervueren Avenue (2004) [3] has discussed some rules as guidelines for Secure Electronic Banking which should be followed and accepted by European Banks. It is very clear that e-banking services and money exchanges build various types of security threats to the banks which should be encountered for security safely. In that report five various type of e-banking services were found which are categorized as five risks? The main idea of this report was to coordinate and guide the banks to use security measurements in e-banking services classified on good practices in view of specific risks. Services advertising are the risk areas which need the use of some specific safety measurements, and the client’s placement and opening need some specific
measurements. A “Know your Customer” requirement is the basic idea for fulfillment of the observance with fund exchanges.

In this discussion there are particular types of the risks covered for the customers dealing in exchange processes. There are the agents or third party service providers who get the banking accounts dealing of customers through their representatives or managers. When we deal with security threats analysis then these give details of the threats or security concerns. In the discussion there are specific notes about managing of other problems which occur time to time.

In this discussion there are advises and steps to be taken by the banks for the coming days in their dealing with the services and applications to Internet. The notes and advise does not mean to be applicable on present issues rather as future scope. These notes as precautions should be applicable when reports give some specific suggestions for Internet services or e-Banking. In 2007 A. Vendor studied the top 10 Internet Business Security threats and these are- phising, kernel attacks and irregularities, internet worms, specific file attacks, window file or format attacks and others.[4].

**Paper CISCO** [5] suggested that commonly the medium sized or lower industries apply the network & Internet usages for finding more clients by providing good services to already present customers in best way. These lower & medium-pacer businesses apply their Internet applications and internet connections to catch new people/clients and new partners on their networks with reduced cost effectively. As the business trend changed on Internet, the high profile hackers took places in these businesses to challenge the security for their benefit. In this scenario more reliable and safe network connections were required. High profile network are required to meet these challenges and to be fit in the framework for the business requirements and providing better services of Internet applications. This reveals that the safety is the largest problem against the lower and mid shaped commerce. This paper describes total 5 security concerns or threats, these are- viruses/ worms, stealing the information, procurement of business, the hidden and rules security [6].

In this discussion it is revealed that new businesses (Medium & lower size) target the new clients or partners using Internet applications on web or network connections. The new threats and
security concern rules are keeping an eye on these business network connections and keep the safety and security of them with due regard of norms and rules. There are the low cost effective security control measures available for these type of businesses which keep the clients authorization genuinely and secured in low cost bearable by them. These maintain the integrity of the system and keep faith of the customers.

CISCO paper discusses that these medium sized business do not care or less care for the security concerns rather they target their attention towards the growth of their business expansions.

There are long tenure plans of Self-Defending Network associated with the Cisco which provide safety and reliability to all actions/access associated with business. This system recognizes, accepts, and stops all types of security concerns/attack.

This Self-Defending Network of CISCO guards these small and medium sized companies in present situations and keeps guard further too. These medium and small sized companies are able to secure their business. They are now able to save their money and costs effectively on network connections. This gives rise to grown up business activities and reduced cost earnings. The paper finds this treatment very cost effective. It is a good for nothing solution for this type of businesses. Hence they are now able to win the faith of the clients and maintain their networks safe and secure.

This Self-Defending Network of CISCO has three specific characteristics which are- 

1. Integration, 
2. Collaboration, and 
3. Adaptability.

First, it integrates security into all elements in the network, ensuring every point in the network can defend itself from both internal and external threats. Second, these network elements work together to exchange information and provide additional protection. Third, the network uses innovative behavioral recognition to adapt to new threats as they arise. The Self-Defending Network of CISCO is a good one solution which reduces the security costs for medium and lower-sized businesses. Thus it makes the self-defending networks more secured.
Sewry & Upfold C.T [7] found that for the Large & lower sized business, the Systems of Information with Technology, paves way for their business along with decision support system. These are the operational conditions associated with them. The SME’s come in link with each and other groups through Internet providing facilities and technologies worldwide and interconnections/networks. The Internet connections and business through emails via e-banking have put their presence in modern world of SME’s. Every business is now accepting Electronic Data Interchange (EDI) and Electronic Businesses (E-Business) for the success and benefit of their business. It is also a fact that these SME’s are not obeying all secured norms. In most cases it is found that the SME’s are avoiding the Security or utilizing only at few layers which is not sufficient. Malicious guarding and backups of data remain aside without testing. In some cases if they plan to implement the Security measurements, then these are not with plans or strategy adoption. There is a unique way of adoption of these controls and measurements that should be done in particular way as standard protocol describes them within their limits. International recognized systems are good and reliable for safety purpose.

Reference:


[2] E-commerce the cutting edge of Business, Bajaj, k. & Nag, TMH [02].


