1.0 Abstract

The important trends of business like supply chain management; non-cash payment, mail order and service economy all are represented by e-Business. The enabling process based upon applications of Internet, Intranets, Extranets or any combination of these as well as related standards of HTML HTTP, XML etc. refers exclusively to e-Business. Basically e-Business stands for internet based business. These share the internet places which have been there kept by companies as routine. This is beyond selling and purchasing. These provide services to clients and companies with associates.

An on-demand e-business is quite flexible responding to all type of fluctuations in the electronic running of the business. This certainly reacts as the actions are taken in an environment. All electronic transactions are anyhow associated and interconnected in demand operating businesses. In this research study we discuss how security should be addressed when transition in electronic business on-demand takes place globally.

This is a hard work of theoretical and practical research work defending against computer virus and designing beneficial computer viruses for efficient processing specially in parallel processing. The damage, attack and detection had been the main research areas till now, but we are asserting our research scope to “limiting of transitivity, functionality, and sharing” is the only \textquoteleft preferred and probably best\textquoteright defenses.

We suggest the results of this analytical work to some stages using analytical study of users doing e-business. In the recent years, attacks on electronic business have drastically grown in dangerous way. The computing resources indulged in e-Business are more vulnerable and heavily dependent on so many things that they become victimized to security threats.

The large information and resource sharing have heightened need for information security. There are security threat concerns about the fund/money transaction securely and electronically. E-Business Policies (e-BP) give integrity, faith and full secured work that can be used for secured Commerce. Theme of the research paper was for study to e-BP techniques as a method
for securing from e-business security threats. This paper is the theoretical survey research paper which aims to specify the benefits of e-Business Policies (e-BP) to provide high security and reducing the negative effects of security concerns on Internet Businesses. An impact of Security Threats has over powered the till now known e-business attacks as the World Wide Web operations and Internetworking increased. When people do online business their data security is on high risk. The personal information in the form of data associated to that business may be compromised in any way. Current solutions to protect Web servers are not comprehensive or robust enough to secure servers and applications from today’s hackers. They still leave systems vulnerable to an ever-growing number of hackers.

Intelligent Attack detection systems (ADS) are being used in e-business today, in order to monitor attempts to break system security. An efficient ADS helps timely detection of security threats and initiation of appropriate countermeasures. A lot of categories of ADS are found in various application areas. Researches are going on in the same field of critical importance to ensure error free continuous services in e-businesses. We present e-Business Attack Detection Systems (e-BADS) through this paper. The utility of the system has been tested on the benchmark database available from UCI Knowledge Discovery in Databases Archive (KDD 2005) and onwards. The results show that the technique is successful for the detection of security threats and attacks in e-business.

Network based attacks on web services associated with e-Businesses are increasing day by day. Network Attack detection systems (NADS) are used in order to monitor attempts to break system security meant for causing security threats to e-Businesses. An efficient NADS helps in detection of security threats and initiation of appropriate countermeasures on e-Business. Many categories of NADS are found in various application areas of networking. Researches are being carried out in this field for ensuring error free service. Many emerging technologies like Intelligent Agents and Artificial Neural Networks etc are proposed by many researchers.

This research paper presents Network Attack Detection System (NADS) for minimizing the negative effects of security concerns on Businesses done on internet. The Online Antivirus Applications (OLAs) impact e-Business activity and individuals’ behaviors. This enhances the
rivalry and business heights and may alter the day to day user’s routine. This research paper includes Security Threats perceived by online users and solving them with NADS. In our study the model analysis and action copying of network threats for the impacts of safety threats on e-business. Threat, loss and cure for e-business safety threats were the targeted scope of this research.

We present the true work of using many fold tools in risk manage in e-business security threats. The work targeted threat modeling was faced by auto produced duplication in system grid threats especially on wide systems which is a common trend there. This work elaborates targeted copying of technology against the impacts of security threats in e-business. Here main concern is to provide a best and total secured electronic environment. Many companies are firing everyday their introductory websites with all possible updates. We tried our best in locating the negative effects and to tackle and deal with them effectively.

We analyzed these effects and searched and tried the possible solutions whether form any technology or system/systems. We applied these to Ten Stage Security Model applicable to the Internet users. These all systems and applications are of no use without considering and making concrete plans and total analysis and testing. There are only limited restrictions available on the security sides to these Industries’ services. We accept that there are many other applications to these businesses that needed very crucial restrictions and tough technologies particularly to deal with customers and money/fund transactions and recoveries. This work has been done for full proof systems and finding the best technologies which may counter with the problems of the users that they face and from the point of their expectations.
2.0 Objective and Scope

The objective of this paper is to look into various aspects and behaviors of the web users doing businesses and money/fund dealings through Internet, then to analyze reports and security concerns with its effects on Trade/Business. There is no perfect security or perfect counter solution to the electronic business concerns.

Security concerns are the main objectives of any e-Business while using the applications allotted for these security concerns. The users doing e-Business faces new challenges which he/she wants to fix while dealing with them. His/Her main concern is to counter with these challenges and odd situations to get total success in e-Business transactions or processes in changed scenario.

We find that there is no full proof or full perfect security while doing e-Business on Internet in its environment. The person/corporate to which the user is dealing can be the fake one or replicating itself. In the changing or rapid processes the IT processes and technologies are the prime responsibilities of the Corporate/Persons so that no failure may take place. Our studies found the security or the strategic model for e-Business and their applications quite useful and successful in dealing with security concerns. Various stages security models and other applications attached with them may solve the faced problems with full responsibilities. While moving to demanding business scenario should be attached with these security steps and technologies because these should ensure full safety in all dealings and transactions.

The analytical study of this work depends upon the various ways by means of which the security concerns or threats can perform losses to the corporate or user while it is supposed that great profits will be made and no loss or security problem will take place. The IT functioning and security systems of e-Business are required to counter with all related problems or security threats otherwise the corporate or user may loose important or confidential data/information. This may put them on stake of reputation. Today the Threats have affected the every aspect of e-business. This paper looks into maximum security concerns to the users doing e-Business. As Internet business is growing day by day its challenges i.e. threats are also growing with it. So the main aim of this study is to know up to which extent it has impact on users and how they are controlled or reduced.
Thus the specific objectives are:

- Recognize different type of security threats and its negative effects to the user doing e-Business. To explore the usage pattern of Internet services.
- How web jobs and their applications work and take place.
- The users doing e-Business may deal with all or maximum security concerns and may able to counter with these problems/hackers.
- Recognize the friendly environment and be ready to deal the fake one.