Protection of e-commerce Using Hybrid Tools

[1]Mohamed Alnuaimi, [1]Mohammad A Al-Fayoumi and [2] Sattar J Aboud
[1]*Middle East University for Graduate Studies, Amman-Jordan*
[2] *Advisor, Iraqi Council of Representatives, Baghdad-Iraq*

Abstract

As long as sensitive data over browsing the net can be the access to the information abuse and to other diseases. Through e-commerce process critical business transactions are transmitted, even entities act online transactions such as banking and shopping over the net and the real threat hangs on the minds of each common individual that is the data transmitted over the Internet is secure. Certainly this is the main question for everyone tries to discover the way out. Each year the organizations spends huge amount to get away from this large threat. There is much more to think where the security issues are concerned but in this paper we will describe the key security solutions. It is very obvious that everyone has an application at various levels when e-commerce and network security is concerned. Therefore we can conclude that there is a need for employing hybrid of these technologies with which we provide 100% security to the e-commerce transactions in order to the public must obtain free idea about net security through transactions.

Keywords: *e-commerce, protection, hybrid, technology, Websites.*

1. Introduction

E-commerce generation situates on the utmost technological revolution that individuals has ever faced the exponential growth of the Internet, lead to look for the latest techniques for conduction successful trade, and trade activities on the Internet. E-commerce is now undergoing a revolutionary stage where the way of communication between the client and the merchant is electronic [1]. The progressive for business today is e-commerce. The e-commerce refers to trading, advertising and marketing products, all these and others are performed over the Internet. In addition the majority of decisions are concerned intimately with business. Consider when e-commerce comes without protection. However, today e-commerce and Internet are work together to increase the efficiency of the entire business [2]. As a result, it is impossible to leave the protection issues. E-ecommerce on the Internet is an actuality online activity, trade, and financial sites and flourishing. The aptitude to control business over the Internet has currently become a need. Unfortunately, doing trade over the Internet will no doubt carry new threats and vulnerabilities. The implementation that select today will expect to alter in the coming years as the business trend alterations. We can assist to choose the e-commerce method that gives the best security and functionality required by both merchants and clients. A few important services that e-commerce is dealing with in daily life such as education, training, medical, and financial transactions on which e-commerce rotates. In general we will divide the e-commerce into three groups of activates [3] which are as follows:

1. Business to Business
2. Business to Commerce
3. Business to Government.

Forresier Research in 2007 reported clearly that the spending on e-commerce services will reach from few hundred million dollars in 1997 to three billions in 2000 and 21 billion via the end of 2007, and a growth of more than 60 times by the end of 2008 [4]. In e-commerce we always create transactions, which might be either receiving records or online transactions over the Internet. On the other words and more specifically business to business e-commerce requires an online environment to authenticate the identity of business groups and to ensure that transactions stay confidential. So, it required a barrier on the network to accomplish the main security aspects such as data integrity, data availability and privacy. The core concept of e-commerce is to reach the flexibility in order to secure the way of client services and payments to be made to all involved participants without compromising on the confidentiality of the partaking agents. Therefore any corporation employing the ideas of e-commerce can be able to find out a large domain to trade with the large number of clients from all over the world.

2. Components of E-commerce

The main components of e-commerce technology [5] are as follows:

1. E-fund transfer

2. E-data interchange
3. E- library
4. E-messaging

In this paper, we will not describe in details these components, but we will attempt to discover the different protection issues and technologies. Considering such a sharp, profitable and multiplier growth provides power to the hackers, pushing via technical challenge for certain financial benefit, providing growth to the cyber crimes. The mysterious diversity of cyber crimes such as hacking, deception during program operations, change data through viruses, tempering with cash distributor, pornography, gambling, spoofing and masquerading, preaching, interception, time theft, unauthorized access, logic bombs, computer sabotage and vandalism, theft of trade secrets and use of online bulletin board for data relating to criminal attacks and attacks related to e-commerce. Currently, many corporations have already implemented e-commerce applications to increase the work opportunity to be implemented at quick rate via making data is common between departments and persons across corporation boundaries. But for these benefits they have to pay the price. However, currently the network is linked to the Internet and this becomes vulnerable to attack via hackers. The CERT Coordination Centre is the main center for reporting Internet security problems. As for each statistics of CERT/CC we can notice the raise of the Internet problems at various levels [6].

Number of events reported

Year	events	**Year**	events
1990	252	2000	21756
1991	406	2001	52658
1992	773	2002	82094
1993	1334	2003	137529
1994	2340	2004	153634
1995	2412	2005	197803
1996	2573	2006	213907
1997	2134	2007	258002
1998	3734	2008	317554
1999	9859		

Total events Reported
(1990-2008) **1458620**

Note that an event may include one site or even hundred of sites. Also, many events may include continuing activity for long intervals of time.

Vulnerabilities reported

Year	**Vulnerabilities**	**Year**	**Vulnerabilities**
1995	171	2002	4129
1996	345	2003	3784
1997	311	2004	5311
1998	262	2005	5877
1999	417	2006	4718
2000	1090	2007	6001
2001	2437	2008	6772

Total vulnerabilities reported
(1995-2008) **41625**

Mail messages processed

Year	**Mail**	**Year**	**Mail**
1990	4448	1999	34612
1991	9629	2000	56365
1992	14463	2001	118907
1993	21267	2002	204841
1994	29580	2003	542754
1995	32048	2004	603344
1996	31268	2005	813555
1997	39626	2006	977801
1998	41871	2007	1233459
		2008	1988511

Total mail messages processed
(1990-2008) **6798349**

Twelve vulnerabilities showed in table 1 below that the most common and most persistent vulnerabilities in the last four years [7]. In drawing up this table, we wanted to highlight the fact that most times hackers do not discover new vulnerabilities but always look for the most common vulnerabilities with the most easily available tools and go for those. This, of course, says a lot about system administrators because these vulnerabilities are very well known with available patches. Yet they are persistently in the top twelve most common vulnerabilities four years in a row. Following is the Department of Homeland Security and SANS/FBI report of last year's top vulnerabilities. U/L in the table stands for UNIX/LINUX operating system vulnerability, and W denotes Windows.

Table 1: Most common vulnerabilities in the last year

Operating System	**Vulnerability**
W	Outlook
W	Internet Information Server (IIS)
W	Microsoft Data Access Components (MDAC)
W	Windows Peer to Peer File Sharing (P2P)
W	Microsoft SQL Server
U/L	BIND (domain name service)
U/L	RPC
U/L	OpenSSL
U/L	SSH
U/L	SNMP
U/L	Apache
U/L	Sendmail

3. **E-security**

The sensitive information over browsing the internet can be the access to the information misuse and to other type of bugs. At some stage in e-commerce control crucial trade transactions are implemented. Even persons perform online transactions such as banking and shopping over the Internet, the real threat holds in each common individual that is the data passed on the network is protected. Certainly, this is the biggest difficulty for each person who tries to find the way out. Each year the corporations spends large amount of money in order to run away from this immense threat. But, we have to identify the kind of information that can be protected; no doubt information can be secured in two types.

1. Information stored on the system.
2. Information sent over the Internet.

In this paper, we will discuss these, but first there are a number of terms which should be obvious to everyone.

Attack: Method of developing vulnerability.
Threats: Interrupt the integrity or functionality.
Vulnerability: Inherent fault caused by inappropriate design.

3.1. E-security Stages

Security given should be:

1. One Passive stage: It is relied on user authentication. The threats in this type are:
   - illegal access
   - Unauthenticated access
   - Spoofing (fabrication or impersonation)
   - Malicious Software
2. Two transmission stage: Main challenges in this type are to give integrity and confidentiality.
   - Interception
   - Modification
   - Repudiation
   - Relay the data

To improve the protection of the on-line transactions encryption and compression are employed for making information unreadable. We can give protection in two various levels.

1. Desktop Level: is known to be the weakest part on the Internet. However, we must limit the user movement by the access control system. This system can be designed to reach the following goals:
   - Allowed persons must obtain access to the desktop.
   - Remove all static passwords to ensure elimination of illegitimate access through logging.
   - Monitoring the part of moving corporation uses on desktop together with their report.
2. Activity level: should contain antivirus programs, firewalls, virtual private network, intrusion detection and vulnerability evaluation together with their best practices. Similar to user and server, access can employ these tools. Antivirus programs and firewalls are working closely to protect the information running out and coming in. In addition, the firewalls are matched with virtual private network, which provides encryption and authentication for remote users of the net. Key issues dodging at the activity level are secure encryption public key infrastructure, authentication, masquerading, and ability without considering the expensive manpower of technology.

3.2. Security Solutions

Before moving to study the technology for the protecting the transactions over Internet one should be certain regarding the answers of the following questions:

1. Do we recognize the risk existing in the Internet?
2. Is the security keystone today enough for the use of the Internet?
3. Is it enough for future foundation?
4. Do we identify the security of the system that constructs information 100% secure?
5. Is the virus protection sufficient?
6. Is the security of the system subjected to an attack?

The general answer is “we have firewalls”. But this answer is not appropriate because of the lack of understanding of security solutions. Individual should know firewalls are just one part of security solutions and they are required to be appropriately configuring and conduct. In addition, it might come under hacking attacks due to the existing bugs in inside the firewall programs. Survey shows that 80% of firewalls are wrongly configured [8]. Therefore we must leave behind the myth of firewalls, and must move to other technologies usually employed. But from the above it is obvious that no individual can provide accurate security solution and pushing to use combination of the technologies. Individual can give security at various levels of the e-commerce transactions over Internet, through communication, authentication, e-mail and web security. The technologies that are in use are as follows:

3.2.1. Cryptography

It is being employed in many security solutions and become a common to give security by broadcast. However, there are two major types of cryptography. The first one is symmetric key which is based on

single key or secret key and the second one is asymmetric or public key which is based on a combination of two keys one for encryption and the other for decryption. Cryptography is being increasingly used to fight off this massive invasion of individual privacy and security, to guarantee data integrity and confidentiality, and to bring trust in global e-commerce [9].

Cryptography has become the main tool for providing the needed digital security in the modern digital communication medium that far exceeds the kind of security that was offered by any medium before it. It guarantees authorization, authentication, integrity, confidentiality, and non-repudiation in all communications, e-commerce and data exchanges in the new information society.

3.2.4 Kerberos Authentication

This is a centralized authentication service that lets both users and severs to authenticate each other and give a secure authentication service in a distributed milieu. Thus it increases flexibility and provides strong authentication framework. However, there are restrictions such as weak password; it will not give any security against password guessing hacks.

Kerberos is a network authentication protocol developed at the Massachusetts Institute of Technology (MIT) and designed to provide strong authentication for client and server applications by using PKI technology. It was designed to authenticate user's requests to the server. In his paper "The Moron's Guide to Kerberos," Brian Tung, using satire, compares the authentication by Kerberos to that of an individual using a driver's license issued by the Department of Motor Vehicles (DMV). He observes that in each case, personal identity consists of a name and an address and some other information, such as a birth date. In addition, there may be some restrictions on what the named person can do; for instance, he or she may be required to wear corrective lenses while driving. Finally, the identification has a limited lifetime, represented by the expiration date on the card.

He compares this real-life case to the working of Kerberos. Kerberos typically is used when a user on a network is attempting to make use of a network service and the service wants assurance that the user is who he says he is. To that end, just like a merchant would want you to present your driver's license issued by the DMV before he or she issues you with a ticket for the needed service, the Kerberos user gets a ticket that is issued by the Kerberos authentication server (AS). The service then examines the ticket to verify the identity of the user. If all checks out, then the user is issued an access ticket [10].

According to Barkley [11], there are five players involved in the Kerberos authentication process: the user, the client who acts on behalf of the user, the key distribution center, the ticket granting service, and the server providing the requested service. The role of the key distribution center is to play a trusted third party between the two communicating elements, the client and the server. The server, commonly known as the "Kerberos server" is actually the Key Distribution Center, or the KDC for short. The KDC implements the Authentication Service (AS) and the Ticket Granting Service (TGS). When a user wants a service, the user provides the client with a password.

The client then talks to the Authentication Service to get a Ticket Granting Ticket. This ticket is encrypted with the user's password or with a session key provided by the AS. The client then uses this ticket to talk to the Ticket Granting Service to verify the user's identity using the Ticket Granting Ticket. The TGS then issues a ticket for the desired service. The ticket consists of the

- requested server name,
- Client name
- Address of the client
- Time the ticket was issued
- Lifetime of the ticket
- Session key to be used between the client and the server

The ticket is encrypted using the server's secret key, and thus cannot be correctly decrypted by the user. In addition to the ticket, the user must also present to the server an authenticator which consists of the

- Client name
- Address
- Current time

The authenticator is encrypted by the client using the session key shared with the server. The authenticator provides a time validation for the credentials. A user seeking server authentication must then present to the server both the ticket and the authenticator. If the server can properly decrypt both the ticket, when it is presented by the client, and the client's authenticator encrypted using the session key contained in the ticket, the server can have confidence that the user is who he claims to be [12].

The KDC has a copy of every password and secret key associated with every user and server and it issues Ticket Granting Tickets so users do not have to enter in their passwords every time they wish to connect to a Kerberos service or keep a copy of their password around.

If the Ticket Granting Ticket is compromised, an attacker can only masquerade as a user until the ticket expires [13]. Since the KDC stores all user and server secret keys and passwords, it must be well secured and must have stringent access control

mechanism. If the secret key database is penetrated, a great deal of damage can occur.

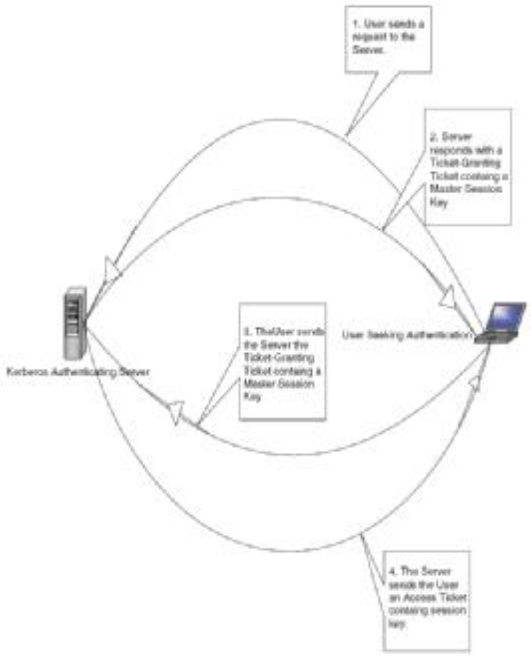

Fig. 1: Kerberos Authentication System

3.2.3 Firewalls

It is a combination of hardware and software that acts together to ensure and to implement the protection policy for the network. But, in fact it does not give hundred percentage securities, which means that it is weaken in the background. For employing firewalls we require to write a suitable security policy. Without the suitable security policy that takes into account many variables that has dynamic characteristics to adapt the constantly altering variants and uses, so firewalls are roughly ineffective. Finally we can state that it can only identify and protect incoming downstream information.

A firewall is hardware, software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network. It is a tool that separates a protected network or part of a network, and now increasingly a user PC, from an unprotected network – the "bad network" like the Internet. In many cases the "bad network" may even be part of the company network. By definition, a "firewall," is a tool that provides a filter of both incoming and outgoing packets. Most firewalls perform two basic security functions:

- Packet filtering based on accepts or denies policy that is itself based on rules of the security policy.
- Application proxy gateways that provide services to the inside users and at the same time protect each individual host from the "bad" outside users.

By denying a packet, the firewall actually drops the packet. In modern firewalls, the firewall logs are stored into log files and the most urgent or dangerous ones are reported to the system administrator. This reporting is slowly becoming real time. We will discuss this shortly. In its simplest form, a firewall can be implemented by any device or tool that connects a network or an individual PC to the Internet. For example, an Ethernet bridge or a modem that connects to the "bad network" can be set as a firewall. Most firewalls products actually offer much more as they actively filter packets from and into the organization network according to certain established criteria based on the company security policy. Most organization firewalls are bastion host, although there are variations in the way this is set up. A bastion host is one computer on the organization network with bare essential services, designated and strongly fortified to withstand attacks. This computer is then placed in a location where it acts as a gateway or a choke point for all communication into or out of the organization network to the "bad network." This means that every computer behind the bastion host must access the "bad network" or networks through this bastion host. Figure 2 shows the position of a bastion host in an organization network. For most organizations, a firewall is a network perimeter security, a first line of defense of the organization's network that is expected to police both network traffic inflow and outflow. This perimeter security defense varies with the perimeter of the network.. See Figure 2.

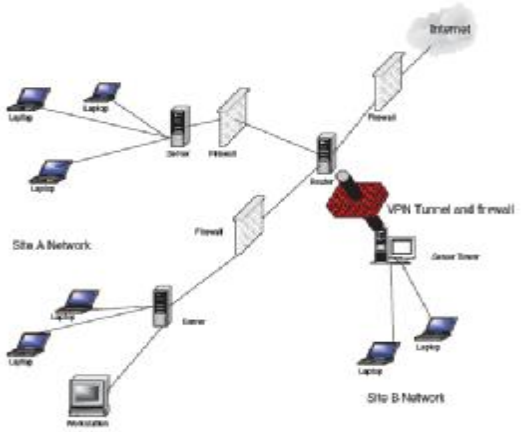

Fig 2: Type of Firewalls

As we pointed out earlier, accept or deny policy used in firewalls is based on an organization's security policy. The security policies most commonly used by organizations vary ranging from completely disallowing some traffic to allowing some of the traffic or all the traffic. These policies are consolidated into two commonly used firewall security policies [14]:

- Deny-everything-not-specifically-allowed which sets the firewall in such a way that it denies all traffic and services except a few that are added as the organization needs develop.
- Allow-everything-not-specifically-denied which lets all the traffic and services except those on the "forbidden" list which is developed as the organization dislike grow.

3.2.4 Intrusion Detection System

Intrusion detection is software and hardware system that monitor a network for malicious activity. This tool is either host based or network based. Intrusion detection system compares network and supply activity with the list of signatures known, to characterize malicious activity. Also, this technology is devoted software applications that exist in a network wire and analyze networks packets. The information encapsulated these packets then compared it with a database of known hack signature, when does not match the packet traffic carries on, if not signal is created. Host based intrusion system has established since the practice of monitoring audit log files. Care with conventional method of searching the complete log files from malicious activity, network intrusion detection system provides an area agent that inspects every activity as an event occurs. It has aptitude to monitor the log files for proof of other attacks. It also has an aptitude to monitor local files for any alterations or revisions.

The notion of intrusion detection in computer networks is a new phenomenon born, according to many, from a 1980 James Anderson's paper, "Computer Security Threat Monitoring and Surveillance." In that paper, Anderson noted that computer audit trails contained vital information that could be valuable in tracking misuse and understanding user behavior. The paper, therefore, introduced the concept of "detecting" misuse and specific user events and has prompted the development of intrusion detection systems.

An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable. The person who intrudes is an intruder. Aurobindo Sundaram [15] divides intrusions into six types as follows:

- Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints. An intrusion detection system for this type is called anomaly-based IDS.
- Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints. These intrusions are also detected using anomaly-based IDS.
- Penetrations of the security control system, which are detected by monitoring for specific patterns of activity.
- Leakage, which is detected by atypical use of system resources.
- Denial of service, which is detected by atypical use of system resources.
- Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

An intrusion detection system consists of several parts that must work together to produce an alert. The functioning of these parts may be either sequential or sometimes parallel [16, 17]. The parts are shown in Fig. 3.

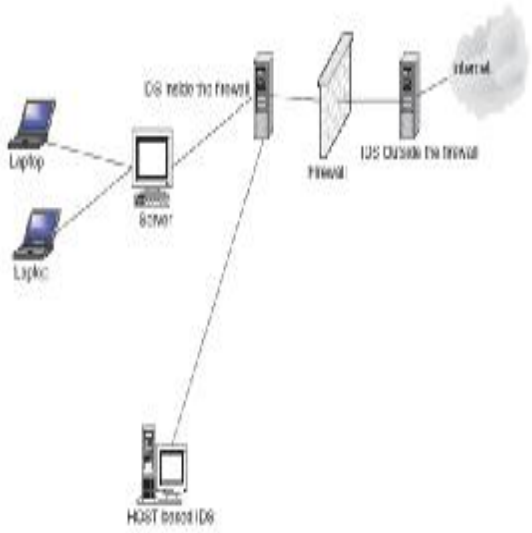

Fig 3: Parts of Intrusion Detection System

3.2.5 Biometric Security

Biometric security is to build or to authenticate persons. This is relied on the methods such as fingerprint, face recognition, retina, and voiceprint. These can be worked by two methods. The registration of features and then identical the stored pattern to real features. Biometric technology, based on human attributes, something you are, aims to confirm a person's identity by scanning a physical characteristic such as a fingerprint, voice, eye movement, facial recognition, and others. Biometrics came into use because we tend to forget something we have. We forget passwords, keys, and cards. Biometric has been and continues to be a catch-all and buzz word for all security control techniques that involve human attributes [7]. Current technology has made biometric access control much more practical than it has ever been in the past. Now, a new generation of low-cost yet accurate fingerprint readers is available for most mobile applications so that screening stations can be put up in a few

minutes. Although biometrics is one of those security control techniques that have been in use the longest, it does not have standards as yet. There is an array of services on the market for biometric devices to fit every form of security access control. Technological advances have resulted in smaller, high-quality, more accurate, and more reliable devices. Improvements in biometrics are essential because bad biometric security can lull system and network administrators into a false sense of safety. In addition, it can also lock out a legitimate user and admit an intruder. So, care must be taken when procuring biometric devices. Before a biometric technique can be used as an access control technique for the system, each user of the system first has his or her biometric data scanned by a biometric reader, processed to extract a few critical features, and then those few features stored in a database as the user's template. When a user requests access to a system resource and that user must be authenticated, the biometric readers verify customers' identities by scanning their physical attributes, such as fingerprints, again. A match is sought by checking them against prints of the same attributes previously registered and stored in the database [3]. One of the advantages that have made biometrics increasingly popular is that while other methods of access control such as authentication and encryption are crucial to network security and provide a secure way to exchange information, they are still expensive and difficult to design for a comprehensive security system.

3.2.6 Virtual Private Network

It offers the way to establish a secure net connection between sites employing the Internet. A virtual private network is basically send data in a secure channel over the entrusted network employing encryption scheme. Virtual private network is reliable for the use of public Internet to send private information between sites. There is another security technique which is at hand instead of virtual private network namely Secure Shell which gives a friendly protocol for security network communication that is less complex and cheaper than hardware relied on virtual private network solution. A VPN is a cryptographic system including Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec that carry Point-to-Point Protocol (PPP) frames across an Internet with multiple data links with added security. VPNs can be created using a single remote computer connecting on to a trusted network or connecting two corporate network sites. In either case and at both ends of the tunnels, a VPN server can also act as a firewall server. Most firewall servers, however, provide VPN protection which runs in parallel with other authentication and inspection regimes on the server. Each packet arriving at a firewall is then passed through an inspection and authentication module or a VPN module Fig 4. The advantages of a VPN over non-VPN connections like standard Internet connections are as follows [18]:

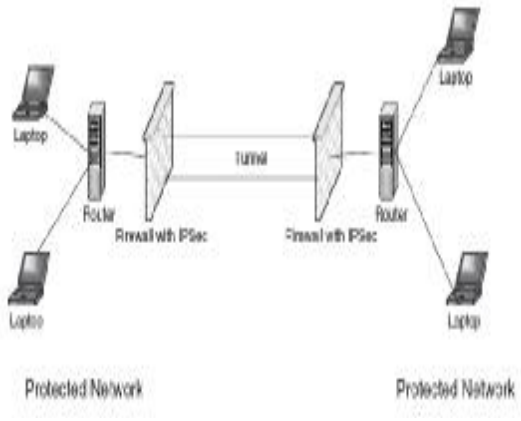

Fig 4: VPN module

- VPN technology encrypts its connections.
- Connections are limited to only machines with specified IP addresses.

3.2.7 Web Security

The fastest growing factor in information technology is Internet based applications and up most requirements is securing the web based applications. SSL (Secure Socket Layer) and TLS (Transport layer Security are the most popular technologies we are having. Along with the new generation of upcoming technology emerging are XML security, security in SOAP and securing the web services framework using .NET and UDDI. SSL: It is a big leap in the direction of providing safe security to the online transactions involving critical information like e-fund transfer and cyber cash. As per survey of world pay e-commerce, 89% of e-commerce users base their decision of purchase of transaction security and 59% on price [19]. But with the increasing trend of e-commerce this ration is changing slowly. During online transaction, it is an event of client or server architecture and is still vulnerable. SSL provides strong solution for security. It is based on the principles of cryptography, authentication, confidentiality, integrity and non-repudiation. The confidentiality is maintained by encryption technology between the two SSL enable pairs. Mainly it contains two sub-protocols, one is SSL that defines format for transmitting data preserving integrity and the second one is SSL handshake protocol defines the steps that lead to decision regarding the choice of session layer. Handshake begins with sending the information like version, cipher setting and other data to the server, which issues digital certificates.

With the increasing traffic, SSL accelerator cards, appliances and servers designed to handle heavy load. SSL cards fitted in the web servers for authentication activities and handle increasing SSL sessions. SSL appliances are fitted to give high performance. These engines are executing complex authentication and key generation activities. Load balancing device is also integrated with appliances. SSL traffic is sent through both and routes all network traffic to the servers. With the sharp growth leads to another SSL solution is "Packetised SSL" developed by Andes Networks. Reports from research organization indicate that the demand for load balances is growing and SSL hardware revenues will touch $595 million with total revenues growing to $1.5 billion by 2009. Along with this the threat is of poor performance on servers leading to a limited number of sessions. SSL and HTTPS are the mechanisms that are typically meant for point-to-point interaction. The advance part of the security of web services is to use new paradigm to SOA (Service oriented architecture) based software, which is more dynamic for developing and deploying these web services. For this we can use SOAP (Simple object access protocol), is easily implemented on other popular protocols. The future foundation of web service security lies is shielding the XML data that flows as a part of SOAP payload. For securing standard XML documents a combination of security standards is to be used (for securing web services) is XML encryption, XML digital signature, XKMS (XML key management services), SAML (Security assertions markup language)

3.2.8 E-mail Security

Most common and most popular application of the Internet is e-mail and it is highly insecure. As during sending, receiving and during modifications the information can be exposed to the hackers at transit time or storage time. There is no lack of standards for secure e-mail such as MIME object security service (MOSS), message security protocol (MSP) and PEM. But the most deployed and popular solution is PGP and S/MIME [20]. The actual operation of PGP as opposed to the management of keys consists of five services: Authentication, confidentiality, compression, e-mail compatibility and segmentation. PGP is the main choice of personnel e-mail where as commercial and industry standards are concerned S/MIME is emerging strongly. As we have seen above, PGP encrypts a message together with the signature (if not sent separately) resulting into a stream of arbitrary 8-bit octets. But since many e-mail systems permit only use of blocks consisting of ASCII text, PGP accommodates this by converting the raw 8-bit binary streams into streams of printable ASCII characters using a radix-64 conversion scheme. On receipt, the block is converted back from radix-64 format to binary. If the message is encrypted, then a session key is recovered and used to decrypt the message. The result is then decompressed. If there is a signature, it has to be recovered by recovering the transmitted hash code and comparing it to the receiver's calculated hash before acceptance.

4. Conclusion and Feature Work

There is much more to think where as security issues are concerned but above are the main security solutions we are having but it is very clear that each has an application at different levels when e-commerce and network security is concerned. Hence we can conclude there is up most need of using hybrid of these technologies or in other words we can say we all need to explore and work on the development of some new technologies with which we give 100% security to the e-commerce transactions so that 89% of the people should get rid of their negative thinking of Internet security during transactions. One should perform the best efforts to stop the most of the attacks along with the use of the technologies are:

1. Employ a Layer 7, full inspection firewall.
2. Automatically update your antivirus at user, server and the gateways.
3. Make all applications and systems updated.
4. Make it sure that you have patched and up to date your server and its applications.
5. Delete all unused programs
6. Turn off all the options of network services, which you are not using regularly.
7. Regularly scan network for common backdoor services using detection.

5. References

[1] Panko, Raymond. R. Corporate Computer and Network Security. Upper Saddle River, NJ: Prentice-Hall, 2004.

[2] Musbah M. Aqel, Sattar J. Aboud and Mohammed A. AL-Fayoumi, Secure Mobile Trade Agent, Journal of Computer Science 3 (5): 329-334, 2007

[3] Gurjodh Singh Dhillon and Jatinder Ohri, Optimizing Security in E-commerce through Implementation of Hybrid Technologies, Proceedings of the 5th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing, Dallas, USA, November 1-3, 2006

[4] Josh Bernoff, New Social Techno-graphics data reveals rapid growth in adoption, Select Forrester research reports 2008.
[5] Sattar J Aboud, And Ghassan Farid Issa, "E-Commerce with Secure Mobile Trade Agent", the 4th Intl. Conference on Computer Science and Information Technology CSIT2006, Amman, Jordan, April 2006. Vol. 3, pp. 300-307.
[6] Computer Emergency Response Team CERT Coordination Center, "*Results of the Security in ActiveX*", Workshop, Software Engineering Institute, Carnegie Mellon University, January, 2009, USA.
[7] Joseph Migga Kizza, a Guide to Computer Network Security, Springer-Verlag, London Limited 2009.
[8] Holden, Greg. Guide to Firewalls and Network Security: Intrusion Detection *and* VPNs. Boston, MA: Thomason Learning, 2004.
[9] Douglas Stinson, Cryptography theory and Practice, CRC Press, 4th Edition 2006.
[10] Brian Tung, the Moron's Guide to Kerberos. www.isi.edu/~brian/security/Kerberos
[11] Barkley, John, Robust Authentication Procedures. http://csrc.nist.gov/publications/ 8007/node166.html
[12] General Information on Kerberos. www.cmf.nrl
[13] Certificate Authentication www.ssh.com
[14] Pipkin, Donald, L. Information Security: Protecting the Global Enterprise, Upper Saddle River, NJ: Prentice Hall, 2000.
[15] Sundaram, A. An Introduction to Intrusion Detection, ACM Crossroads: Student Magazine, Electronic Publication. www.acm.org/crossroads/xrds2–4/intrus.html
[16] Proctor, P., the Practical Intrusion Detection Handbook, Upper Saddle River, NJ: Prentice Hall, 2001.
[17] Innella, P., the Evolution of Intrusion Detection Systems, Tetrad Digital Integrity, LC. http://www.securityfocus.com/infocus/1514
[18] Kizza, J. M., Computer Network Security and Cyber Ethics, McFarlans Publishers, Jefferson, NC: 2002.
[19] Byers, Simon, Juliana Freire, and Cl̀udio Silva, Efficient Acquisition of Web Data through Restricted Query Interfaces. AT&T Labs-Research, www10.org/cdrom/posters/p1051
[20] NASA World Wide Web Best Practices 2000–2001 Draft Version 2.0. www.nasa-wbp.larc