



Network Security and its importance

Krithika

Department of Information Technology
Saveetha School of Engineering, Chennai, India

Abstract: Network protection has come to be extra vital to confidential users, associations, and the army sources. The uses of the internet, protection came to be a main concern and the past of protection permits a larger understanding of the rise of protection technologies. The design of the internet, after adjusted can cut the probable aggressions that can be dispatched across the network. There are a colossal number of confidential, businesses, martial. Power data on networking infrastructures worldwide countless companies safeguard. Knowing attack methods permits for the appropriate protection to emerge. The center earth of web protection is large. The scope of discover encompasses brief recovery back to internet's origins. The companies craft an "intranet" tore main related to the internet but safeguarded from probable threats. With regard to comprehend scrutiny been given nowadays, behind view of the net, consequently revised.

I. Introduction

The advent of the Internet and new networking technology is becoming more interconnected with the world. Network security has become a great importance these days. The system of network security typically relies on layers of protection and consists of multiple components. Entire components work together to increase the overall security of the computer network. The data network has considered an internet. The computer based data consists of latest information, which can be obtained by Trojan horses. Data networks and synchronous network comprised of switches are the two different networks. Web synchronous consists of switches does not buffers the data's and consequently are not intimidated by attackers.

The following are the web protection:

- Protection of history in networks.
- The aspects of the Internet are architecture and vulnerable protection.
- Kinds of internet aggressions.
- Web protection and internet access.

Present progress in web protection on hardware and software. There exists a "correspondence hole" between the engineers of security innovation and designers of systems. This offers seclusion, adaptability, ease-of-use and institutionalization of conventions. The conventions of diverse layers could be effortlessly joined to make stacks which permit measured improvement. The execution of distinctive layers might be changed later without making different alterations, permitting adaptability being developed.

On considering network security, it must be emphasized that the whole network is secure. When transmitting data the communication channel should not be vulnerable to attack. As opposed to system outline, secure system configuration is not a well- created procedure. There isn't a system to deal with the many-sided quality of security necessities. Secure system outline does not hold the same focal points as system configure. When growing a safeguard web, the pursuing demands was believed (1): Accessing—the way to converse the authorized accounts from a particular network. Confidentiality—the web holds private information. Verification process—identifying the individuality. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. These instruments are encryption, authentication mechanisms, intrusion-detection, protection association and firewalls. To less the vulnerability of the computer to the web there are countless produce available. Companies across the globe are employing a combination of a little of these tools. "Intranets" are both related to the internet and reasonably protected from it. Understanding the protection subjects of the internet considerably assists in growing new protection technologies and ways for webs alongside internet admission and internet protection itself. The internet design itself leads to vulnerabilities in the network. Intrusion detection arrangements are established on the kinds of aggressions most usually used. The kinds of aggressions across the internet demand to additionally be learned to be able to notice and guard opposing them. Web intrusions encompass of segment gives caution for the pursuing statements:

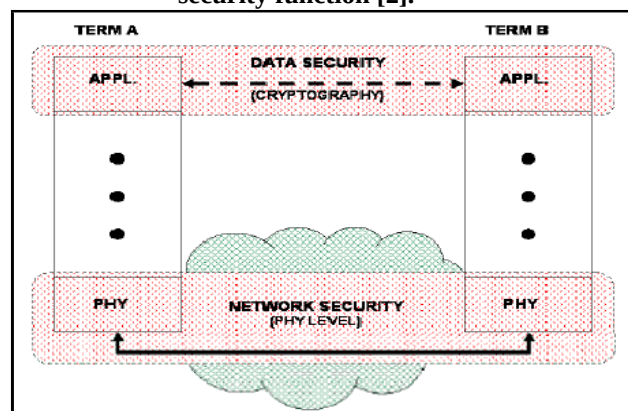
- To obtain resources uselessly,
- Inhibit alongside each arrangement resource's aimed function,
- To gain arrangement vision that is flaw in afterward attacks. The final reason for a web intrusion is most usually guarded opposing and believed by most as merely as motive.

Typical protection presently exists on the computers related to the network. The layers of the protection ideal correspond to the Open System Interconnections ideal layers Protection protocols from time to time normally materialize as portion of a solitary layer of the Open System interconnections web reference model. This protection way leads to a competent and effectual design that circumvents a little of the public protection problems. Current work is being given in employing a layered way to safeguard web design.

II. Differential Data and Network Security

Data is the aspect of protection that permits a client's data to be transformed into unintelligible data for transmission purpose. Technical methods have to tolerate to advance due to the advancement of the hackers as well. A key is demanded to decode the message. Forceful cryptography and Solid cryptography in the past might be efficiently broken today. A harmless arrangement will likewise retain somebody from embeddings unapproved memos into the system. At the point after exchanging figure memo above an arrangement, it is functional to have a harmless system. This will seize into thought the figure content to be safeguarded, alongside the aim that it is extra improbable for a little people to even endeavor to break the code. Subsequently, hard figures are needed and forceful arrangements [2].

Figure 1: Based on the OSI model, data security and network security have a different security function [2].



Therefore the application writers are aware of its existence. The relation of network security and data security to the Open System Interconnection model is shown in Figure 1. The user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. Layers above the physical layers are also used to accomplish the network security required [2].

III. HISTORY OF NETWORK SECURITY

Modern attention to insecurity was an offence committed by Kevin. He committed the biggest computer-related offence in United States history [3]. Since then, data protection came into the spotlight. The damages were 80 million dollars in United States intellectual property and basis program from a collection of companies' public web pages being laid on to hold commercial and confidential materials. The progress of details that is made obtainable across the internet, data protection additionally needed to evolve. Inside the contact stack, protocols for protection are not implemented. Internet protocols in the past were not industrialized to safeguard themselves. Current events in the internet design have made contact extra secure. This leaves the internet open internet system.

A. History of Internet

Origin of internet comes from the year 1969, Elevated Scrutiny Undertakings Association Web (Arpanet's) commissioned by the department of protection of scrutiny in network. The Advanced Research Projects Agency Network is an accomplishment from the extremely beginning. Vinton selected the early chairman of the International packet Working Group, and afterward becomes recognized as a "Father of the Internet." [10]

The Inter Networking Working Cluster becomes the early countless standards-setting entities to law the producing web. In the 80s, Bob Vinton key associates of a team that craft Transfer Communication Protocol/Internet Protocol, the public speech of all Internet computers. The blending of in unreasonable desktop mechanisms and capable, network-ready servers permit countless associations to link the Internet surprisingly.

The Globe Expansive Web was born. Netscape and Microsoft were both contesting on growing a browser for the internet. In the 90's, the internet started to come to be obtainable to the public. Internet endures to produce and surfing the internet has come to be equivalent to TV thinking for countless users. The mid-80s marks a boom in the confidential computer and super-minicomputer industries. The combination of in luxurious desktop mechanisms and influential, network-ready servers permits countless firms to link the Internet for the early

time. In the 1990s, the internet began to become available to the public. Internet continues to grow and surfing the internet has become equivalent to TV viewing for many users.

B. Security Timeline

The timeline can be started as far back as the 1930s. Securing communications was essential in World War II. Several key events contributed to the birth and evolution of computer and network security. Polish cryptographer created an engine machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing; a brilliant mathematician broke the code for the Enigma.

In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology (MIT) students. During the 1970s, the Telnet protocol was developed. The Department of Defense field began the ARPA Net, which gains popularity as a conduit for the electronic exchange of data and information.

During the 80s, the hackers and offenses associating to computers were commencing to emerge. The 414 gang are raided by powers afterward nine-day cracklings preen whereas they break into top-secret systems. The Computer Fraud and Mistreatment Deed of 1986 were crafted because of Ian Murphy’s offense of robbing data from martial computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to above 6,000 vulnerable computers related to the Internet. Past times tells about Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide [3]. On any day; there are approximately 225 major incidences of a security breach. Investment in proper protection ought to be a priority for colossal associations as well as public users. These protection ruptures might additionally consequence in monetary defeats of a colossal degree.

IV. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

These protection mechanisms permit for the storing of details that are transferred across the network. The Internet Engineering Task Power (IETF) has given protection mechanisms at assorted layers of the Internet Protocol Suite [4] protection design of the internet protocol, recognized as Internet Protocol Security, is a standardization of internet security. Internet Protocol protection, Internet Protocol sector, covers the new creation of Internet Protocol (IPv6) as well as the present edition (IPv4). Even though new methods, such as Internet Protocol Section have been industrialized to vanquish net’s deficiencies, which are insufficient [5]. Figure 2 displays a discernible representation of how Internet Protocol section is requested to furnish safeguard communications. Internet Protocol Section can be utilized as transport mode and tunnel mode. Internet Protocol Section is the supplementary decoder to allocate key or keys. These aggressions are analyzed to ascertain supplementary protection mechanisms that could be necessary. Even though protection could continue inside the protocol, precise aggressions cannot be guarded against.

A. IPv4 and IPv6 Architectures

The main parts of the architecture relating to security are discussed in detail.

The IPv4 displayed countless limitations afterward two decades [6]. The IPv6 protocol was projected alongside IPv4’s shortcomings in mind. The main parts of the architecture relating to security are discussed in detail. The protection design of the internet protocol, recognized as Internet Protocol Security, is a standardization of internet security. Internet Protocol protection, Internet Protocol sector, covers the new creation of Internet Protocol (IPv6) as well as the present edition (IPv4). Even though new methods, such as Internet Protocol Section have been industrialized to vanquish net’s deficiencies, which are insufficient [5]. Figure 2 displays a discernible representation of how Internet Protocol section is requested to furnish safeguard communications.

Internet Protocol Section can be utilized as transport mode and tunnel mode. Internet Protocol Section is the supplementary decoder to allocate key or keys.

These aggressions are analyzed to ascertain supplementary protection mechanisms that could be necessary. Even though protection could continue inside the protocol, precise aggressions cannot be guarded against.

B. IPv4 and IPv6 Architectures

The main parts of the architecture relating to security are discussed in detail. The Internet protocol version 4 displayed countless limitations afterward two decades [6]. The internet protocol version 6 alongside IPv4’s shortcomings in mind. The main parts of the architecture relating to security are discussed in detail.

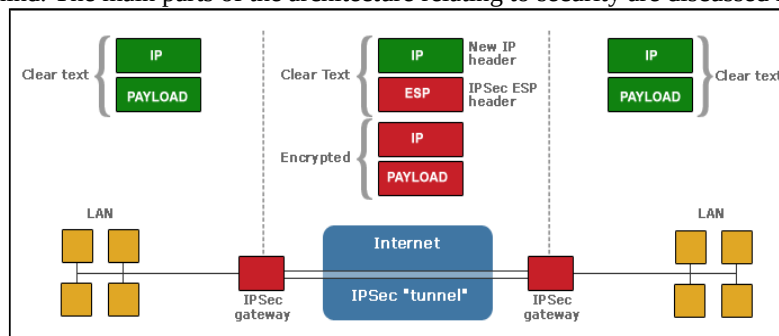


Figure 2: It encompasses a gateway and a tunnel order to safeguard communications [17].

A.1 Internet Protocol version 4 Architecture

The protocol encompasses a couple aspects that provoked setbacks alongside its use. They are remarked to gain a comprehensive understanding of the internet protocol and its shortcomings. These setbacks do not all associate to security. The reasons of the protocols are: Address Space, Routing, Configuration, Security, Quality of Service.

This architecture has an address that is 32 bits expansive [6]. The setback of exceeding that number was not predictable after the protocol was created. The tiny address space of the IPv4 facilitates malicious program allocation [5]. This limits the maximum number of computers that can be related to the internet. The 32 bit address provides for a maximum of two billions computers to be related to the internet. But, the problems for routing in protocol is because of the tables are constantly increasing in size. Methods have been adopted to reduce the number of entries in the routing table. The maximum theoretical size of the global routing tables was 2.1 million entries [6]. This eases the configuration has less for the user but not the network's administrators. Mechanisms to secure Internet Protocol version 4 do exist, but there are no requirements for their use [6]. The form of protection does not account for the skilled hacker. Internet Protocol section is a specific mechanism used to secure the protocol. Internet Protocol section secures the packets loads by means of cryptography, the services of confidentiality, integrity, and verification. Some of the information required is the IP address, routing gateway address, subnet mask, and Domain Name System server. The simplicity of configuring the network is not evidencing the Internet Protocol version 4.

A.2. Internet Protocol Version 6 Architecture

This version was being developed to emphasis the aspects of the Internet Protocol version 4 that needed to be improved. The improvement steps are placed in the following areas:

- Routing & addressing,
- Multi-protocol architecture,
- Security architecture,
- Traffic control,

The address bits have used less efficiently for this protocol because it simplifies addressing configuration. The IPv6 routing arrangement is supplementary effectual and enables tinier globe routing tables. Hosts can automatically configure themselves. This new design permits ease of configuration for the user as well as web administrator. The host configuration is additionally simplified. The protection design of the IPv6 protocol is of outstanding interest. IPSec is embedded inside the IPv6 protocol. IPSec functionality is the alike for IPv4 and IPv6. The only difference is that IPv6 can use the protection mechanism alongside the whole path [6]. The internet protocol permits for distinct precise packets for higher quality of service.

B. Attacks through the Current Internet

Internet Protocol Version 4

There are four attributes for system protection, which were remarked beforehand in a somewhat desperate form, but are restated for ease and emphasis. The protection qualities are Confidentiality, Privacy, Integrity and Availability.

Privacy and integrity yet grasp to the definition. Privacy is the right to protect confidential secrets and information.

Different kinds of attack ways associate to these four protections attributes. The computer system assets can be accessed by authorized people.

Table (1) shows the offensive methods and safety.

Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, Hacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

The current technology for dealing these attacks is understood in order to comprehend the current research developments in security hardware and software. Not all of the methods in the table above are discussed.

B.1 Common Internet Attack Methods

Common internet aggressions methods are broken down into categories. A little aggressions gain arrangement vision or confidential data, such as eavesdropping and phishing. Supplementary forms of web intrusions additionally continue, such as earth aggressions, smurf aggressions. Those aggressions are not as well recognized as DOS aggressions. But they are utilized in a little of time. Attacks can additionally inhibit alongside the system's aimed purpose, such as worms, malware, Trojans and viruses.

B.1.1 Eavesdropping

Block endeavor of correspondences by an unapproved meeting is shouted spying. Remote spying is the point at that the individual just furtively listens to the coordinated messages. Next once more, vibrant spying is the point at that the interloper listens and supplements something into the correspondence stream. This can punctual the memos being mutilated. Fragile data might be stolen thusly [8].

B.1.2 Viruses

Viruses are self-replication plans that use files to infect and propagate [8]. Once a file is opened, the virus will onset inside the system.

B.1.3 Worms

There are two main kinds of worms, mass-mailing worms and network-cognizant worms. Mass mailing worms use email as a way to infect supplementary computers. The worm does not need a file to permit it to propagate [8]. Network-aware worms are a main setback for the Internet. A network-aware worm selects a target and after the worm accesses the target host, it can infect it by way of a Trojan or otherwise.

B.1.4 Trojans

Trojans normally hold a little wage burden such as a virus [8]. Trojans materialize to be benign plans to the user, but will truly have a little malicious purpose.

B.1.5 Phishing

The process of attaining confidential data from a group or association [9]. Phisher's mislead users into disclosing personal data, such as trust card numbers, online bank system, credentials and supplementary sensitive information.

B.1.6 IP Spoofing Attacks

The intruder is hidden by disparate way making detection and prevention difficult. With the present IP protocol knowledge, IP- spoofed packets cannot be eliminated [8].

B.1.7 Denial of Service

Denial of Service is an attack after the arrangement consenting too countless demands cannot revisit contact alongside the requestors [9]. Eventually, the arrangement cannot answer to each extra demands portray ignite lacking service. The arrangement next consumes resources staying for the handshake to complete.

B.2 Technology for Internet Security

Disparate protection and detection mechanisms were industrialized to deal alongside these attacks.

Internet menaces transferred across the Internet.

B.2.1 Cryptographic systems

It encompassed the use of codes and ciphers to change data into unintelligible data. Cryptography is defined as the functional and extensively utilized instrument in protection engineering today.

B.2.2 Firewall

The intention of firewall catalog block traffic from the beyond, but it might additionally be developed filter systems known as packet filter firewalls. It is the system that prevents unauthorized access to or from a network. They can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent the unauthorized internet users from accessing. It is an arrangement project to stop unauthorized admission to or from a confidential browser. Servers can be requested in both systems and multimedia, or even the combination of them [8].

B.2.3 Private Network Detection Systems

Intrusion Detection Systems arrangements have made in multimedia and hardware mechanisms to notice an attack. IDS produce to utilize the monitor connection in ascertaining aggressions have been launched.

B.2.4 Anti- Software and scanners

Distinct so-called Anti-Malware instruments provide to notice the remedy for an infected system.

Viruses, Worms, and Trojan horses are few examples of malicious multimedia.

B.2.5 Secure Socket Layer (SSL)

Secure Socket Layer is projected to craft a safeguard channel, or tunnel, a web browser and the web server, so that each data exchanged is protected inside the safeguarded tunnel. SSL provides verification of clients to server across the use of certificates. Clients present a certificate to the server to clarify their identity. The average method is to accomplish a good level of protection of a web browser and a website.

C. Security Issues of IP Protocol IPv6

From a protection point of view, IPv6 is a substantial advancement above the IPv4 internet protocol. Although the IPv6's outstanding protection mechanisms, it yet endures to be vulnerable to threats. Some Areas of the IPv6 protocol yet pose a possible protection issue. The fresh internet protocol does not protect opposing mis-configured server are poorly projected requests, or poorly protected sites. The possible security problems emerge due to the following [5]:

- Header manipulation issues,
- Flooding issues,
- Mobility issues.

The development headers demand to be processed by all stacks, and this can lead to a long shackle of development headers. Spoofing endures to bear protection menace on IPv6 protocol. The colossal number of expansion headers can overwhelm precise node and is a form of attack iritic deliberate. The feature needs distinct protection measures. Web administrators demand to be cognizant of the protection needs after employing IPv6's mobility feature.

V. SECURITY INDIFFERENT NETWORKS

Nowadays the companies use combinations of encryption and authentication mechanisms to craft "intranets". That are usually related to the internet but protected from it at the time. Intranets differs among "Extranets" in the preceding are usually confined to operatives for the association as private network is usually accessed by various trade personalities. Later admission is endowed it is normally across a gateway alongside safeguard, user verification, encrypt memos. Even though they have designed swiftly to allocate details in manipulated nature is that taut security. Failure of a closed restricted private network is that vital details could become the labor satisfaction. A private network have local inside brokers. For broader details allocation, they could retain larger guards: Unauthorized access and report illegal entry, Silent alteration or destroying by checking the unauthorized access, Authorized laws for agent onset of Email connections, Encryption process for associations and information exchanges, Timed password or assurance declarations. Private browsing that continues across several locations usually run above distinct leased lines or answer way of Virtual Private Network can be utilized. Virtual Network is a confidential web that uses an area web (usually the Internet) to link remote locations.

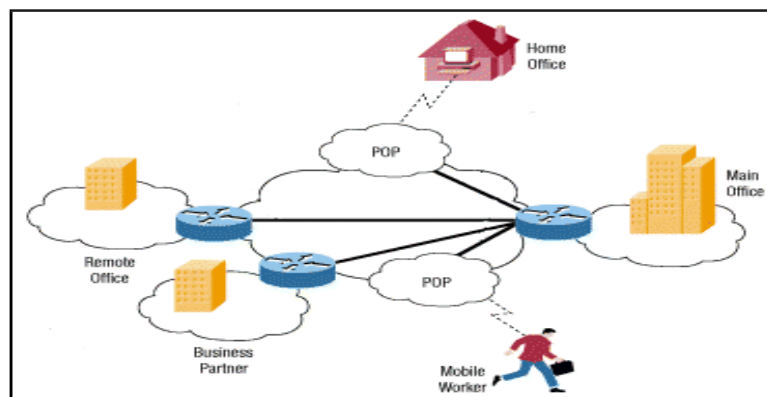


Figure3: A normal Virtual Private Network has a main Local Area connection at the company head office of a firm, supplementary Local Area Network's at remote workplaces or abilities and single users relating from out in the field. [14]

VI. CURRENT STATUS IN NETWORK SECURITY

Web protection earth tolerates. This could considerably cut the unauthorized admission of safeguard machines. New technique like the intelligent chip surf on web security. It provides a method of authentication process than passwords the multimedia aspect of web protection is extremely dynamic. Scrutiny gives present progress and upcoming events of the field.

1. Circuits and system Developments

These days central processing units are not developing rapidly. Microchip system is the only new system technology that is widely impacting security. The most pleasing use of biometrics for web protection is for safeguard work station logons for a work station related to a network. Every workstation needs a small multimedia prop for biometric identification of the user as well as, a hardware device. The price of hardware mechanisms lead to the extensive need of voice biometric protection identification on low budget. Hardware mechanism such as computer mice rafted in thumb print readers should be the subsequent pace up. These mechanisms should be extra luxurious to apply on countless computers; a find contraption should need its own

hardware device. The supremacy of voice credit multimedia is that it can be centralized, therefore cutting the price of implementation each machine. At top of the scope a centralized voice biometric package can price up to 50,000 dollar but could be able to grasp the safeguard of 5000 machines.

Current system of analyzing biological network security will be tore place the current password system. Passwords have to be changed every few months. Out of the system by in correctly entering their password repeatedly. Very often people write their password and keep it near to their computer. This is of course completely undermines any effort at network security. Biometric can modify this confidential security method. The use of biometric security avoid this problem whereas it is expensive to setup at the beginning these devices save administration and user assistance costs. The card is designed to store encryption keys.

The main idea behind microchip is to provide acceptable proof of a user's identity. Microchip can be used for everything from logging into the network to provide secure Web communications and to secure-mail transactions. Those microchips are nothing more than a repository for storing passwords. Fortunately, there are protection features crafted into intelligent cards to stop someone from employing as token card. Intelligent cards need anybody who is employing them to go in a confidential identification number (PIN) beforehand they will be conceded each stages of admission into the system. The Personal Identification Number has comparable for the Personal Identification Number utilized by ATM machines. This Personal Identification Number was allocated to the user by the administrator at the period the administrator delivered the card to the user.

Due to the Personal Identification Number is short and purely numeric, the user have no trouble in remembering it. It is confirmed from inside the intelligent card. Because the Personal Identification Number is not ever sent across the web, there's definitely no danger of it being intercepted. The main benefit, nevertheless, is that the PIN is unusable lacking the intelligent card, and the intelligent card is unusable lacking the PIN. It allocates the user by the administration to deliver the card to the user.

2. Software Developments

The aspect for the web protection is extremely vast. It adds up firewalls, antivirus, intrusion detection, and far more. The enhancement of the average protection multimedia yet stays the same. This procedure is the alike for firewalls and intrusion detection systems. As protection hardware transitions to biometrics, the multimedia additionally needs to use the data appropriately. Countless scrutiny papers have been skimmed were established on analyzing attack outlines in order to craft matter protection software. Current scrutiny is being given on protection multimedia employing neural networks. The goal of the scrutiny is to use neural webs for the facial credit multimedia. Most of the present protection algorithms are computation al intensive and need comprehensive processing power. Countless tiny earth convoluted mechanisms can be related to the internet. This domination, though, is not obtainable in tiny mechanisms like sensors. Therefore, there is a demand for arranging light-weight protection algorithms. Scrutiny in this span is presently being performed.

VII. FUTURE TRENDS IN SECURITY

The immune arrangement fights off aggressions and builds itself to battle tougher enemies. The upcoming will perhaps be that the protection is comparable to an immune system. The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

VIII. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. Originally it was consented about the significance of the web protection earth, new ways to protection, both hardware and multimedia, should be actively researched. The embedded protection of the modern internet protocol IPv6 could furnish countless benefits to internet users. This technology is mostly software based, but many common hardware devices are used. Even though a little protection subjects were noted. The IPv6 internet protocol seems to evade countless of the present accepted attacks. The web protection earth could have to evolve extra quickly to deal alongside the menaces more in the future. It was a surprise to discern most of the progress seizing locale in the technologies being presently used.

REFERENCES

- [1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *Computer*, vol.31, no.9, pp.24-28, Sep 1998.
- [2] Kartalopoulos, S.V., "Differentiating Data Security and Network Security," *Communications*, 2008. *IEEE International Conference on*, pp.1469-1473, 19-23May2008
- [3] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.
- [4] Molva, R. Institute Eureka, "Internet Protection Architecture," in *Computer Networks & ISDN Arrangements Journal*, vol7.
- [5] Sotillo, S., East Carolina University "IPv6 protection issues", Aug/2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.
- [6] Andress J. "IPv6: the next internet protocol," April2005" www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.
- [7] Warfield M., "Security Implications of IPv6," *Internet Security Systems White Paper*, documents.iss.net/whitepapers/IPv6.pdf
- [8] Adeyinka, O., "Internet Attack Methods and Internet Protection Technology", "Modeling & Simulation", In 2008.

- AICMS08.Second Asia Global Session on,vol., no., pp.77-82, 13-15May2008
- [9] Marin, G.A., "Network security basics, "*Security& Privacy, IEEE*, vol.3, no.6, pp.68-72, Nov.-Dec.2005
- [10] "Internet History Timeline," [www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm](http://www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.htm).
- [11] Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access, "*Proceedings of the IEEE*, vol.85, no.12, pp.2034-2051, Dec1997
- [12] "Intranet."*Wikipedia, the Free Encyclopedia*.23Jun2008, 10:43UTC.Wikimedia Foundation, Inc.2 Jul2008<<http://en.wikipedia.org/w/index.php?title=Intranet&ol did=221174244>>.
- [13] "Virtual private network."*Wikipedia, the Free Encyclopedia*.30Jun2008, 19:32UTC. Wikimedia Foundation, Inc.2/Jul/2008<http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>.
- [14] Tyson, J., "How Virtual private networks work,"<http://www.howstuffworks.com/vpn.htm> .
- [15] Al-Salqan ,Y.Y., "Future trends in Internet security," *DistributedComputingSystems*,1997.,*Proceedings of the Sixth IEEE Computer Society Work shop on Future Trends of*, vol.,no.,pp.216-217,29-31Oct1997
- [16] Curtin. "Introduction to Network Security,"<http://www.interhack.net/pubs/network-security>.
- [17] "Improving Security,"http://www.cert.org/tech_tips, 2006.
- [18] Serpanos, D.N.; Voyiatzis, A.G., "Secure network design: A layered approach, "*Autonomous Decentralized System, 2002.The 2nd International Work shop on*, vol., no., pp.95-100, 6-7Nov.2002
- [19] Ohta, T.; Chikaraishi, T., "Network security model"*Networks, 1993.International Conference on Information Engineering'93*'. "*Communications and Networks for the Year2000*", *Proceedings of IEEE Singapore International Conference on*, vol.2, no., pp.507-511vol.2, 6-11Sep1993, l.31, pp.787-804, April 1999.