Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Methods of Network Security and Improving the Quality of Service – A Survey

Purna Chandra Sethi
PhD Scholar, Dept. of Computer Science
Utkal University
Bhubaneswar, India

Prafulla Kumar Behera
Reader, Dept. of Computer Science
Utkal University
Bhubaneswar, India

Abstract— In current scenario, almost all operations are performed over Internet. Networking services are highly adopted by the current human race. All types of services are available at finger tips. Network services are extremely important because many companies provide their services over the Internet. Hence, there is a high demand for security in managing the information along with faster processing of the operations. Due to the enormous demand for network services, the performance of these services has to be improved. Along with this increased demand for network services, numbers of unfair activities by the hackers are also increasing at an exponential rate, which must be controlled for protecting information. This increase in the amount of important information increases the packet payloads, which in turn leads to implementation of load balancing, so that the related network operations can be performed effectively. Hence, there is genuine demand for improving the quality of services so that the processing becomes faster. In this paper, we have made a brief study of the network security issues, along with the methods of faster network services for improving the quality of services.

Keywords— Network security, Data Security, Network attacks, QoS

I. INTRODUCTION

Network security has become more important to personal computer users, organizations, and the military. With the advent of the Internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the Internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to be applied. Many businesses secure themselves from the Internet by means of firewalls and encryption mechanisms. The businesses are developed to remain connected to the Internet as well as secure the information from possible threats.

The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to Internet's beginnings and the current development in network security. In order to understand the current research trend, background knowledge of the Internet, its vulnerabilities, attack methods through the Internet, and security technology is important and therefore they are reviewed.

The world is becoming more interconnected with the advent of the Internet and new networking technology. Large amount of personal, commercial, military and government information depends on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the Internet.

There are currently two fundamentally different networks present, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses", placed in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the Internet, and other networks that link to the internet.

The vast topic of network security is analysed by researching the following:

1. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of Internet attacks and security methods
4. Security for networks with Internet access
5. Current development in network security hardware and software

Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand where network security is heading.

1.1. Network Security

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the TCP/IP model. The TCP/IP model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well developed process. It is in a growing stage. There is no proper methodology developed to manage the complexity of security requirements.

Secure network design does not contain the same advantages as network design. When considering network security, it must be emphasized that the whole network is secure. Network security does not concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of authenticity (identity) for accessing the network
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refuse that he used the network

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. The steps involved in understanding the composition of a secure network, Internet or otherwise, are followed throughout this research endeavor.

To reduce the vulnerability of the computer to the network, there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. The Internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the Internet greatly assists in developing new security technologies and approaches for networks with Internet access and Internet security itself.

The types of attacks through the Internet also need to be studied to be able to detect and guard against them. Based on the most commonly used attacks, Intrusion detection systems are established. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource intended function
- To gain system knowledge that can be exploited in later attacks

Security protocols usually appear as part of a single layer of the TCP/IP network reference model. Current work is performed using a layered approach to secure network design. The layers of the security model correspond to the layers of TCP/IP model. This security approach leads to an effective and efficient design which solves some of the common security problems.

1.2. Differentiating Data Security and Network Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well.

When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed [1].

The relationship of network security and data security to the TCP/IP model is shown in Figure 1. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. 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 [1]. Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent countermeasure strategies [1].

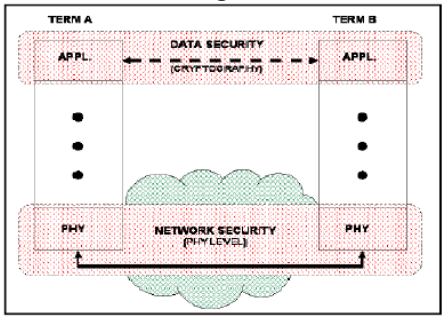

Figure 1: Based on TCP/IP model Data Security and Network Security have different security Function [1]

II. HISTORY OF NETWORK SECURITY

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in U.S. history [2]. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies [2]. Since then, information security came into the spotlight. Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the Internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies emphasize security for the intellectual property.

Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the Internet open to attacks. Modern developments in the Internet architecture have made communication more secure.

2.1. Brief History of Internet

The birth of the Internet takes place in 1969 when Advanced Research Projects Agency Network (ARPANet) is commissioned by the department of defence (DOD) for research in networking. Although originally designed to allow scientists to share data and access remote computers but e-mail becomes the most popular application among all. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. Vinton Cerf is elected the first chairman of the INWG (International Network Working Group), and later becomes known as a "Father of the Internet". For this reason, he was awarded the most prestigious Turing award.

In the 1980s, Bob Kahn and Vinton Cerf developed the TCP/IP model. So, the loose collection of networks which made up the ARPANET is coined as "Internet". The mid-80s marks a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful network-ready servers allows many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers.

In the 1990s, the Internet began to become available to the public. The World Wide Web was born. Netscape and Microsoft were both competing on developing a browser for the Internet. Internet continues to grow and surfing the Internet has become equivalent to TV viewing for many users.

2.2. Security Timeline

Several key events contributed to the birth and evolution of network security. The timeline can be started as far back as the 1930s. In 1918, cryptographers created an enigma machine that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War I and advanced coded structure in World War II by German military.

In the 1960s, the term "hacker" is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defence began the ARPANet, which gains popularity as a conduit for the electronic exchange of data and information. During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers [2].

During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking where they break into top-secret systems. Due to Ian Murphy's crime of stealing information from military computers, the Computer Fraud and Abuse Act of 1986 were created. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000 vulnerable computers connected to the Internet.

Based to the problems generated due to Morris Worm, the Computer Emergency Response Team (CERT) was created that will alert computer users of network security issues. In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the Internet today worldwide. On any day, there are approximately 225 major incidences of a security problem. These security problems could also result in monetary losses in large degree. Investment in proper security should be a priority for large organizations as well as common users.

III. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite. These security mechanisms allow for the logical protection of data units that are transferred across the network. The security architecture of the internet protocol, known as IP Security, is a standardization of Internet security. IP security covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome Internet's best-known deficiencies, they seem to be insufficient [3]. IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes [4].

The current version and new version of the Internet Protocol are analysed to determine the security implications. Although security may exist within the protocol, certain attacks cannot be guarded against. These attacks are analysed to determine other security mechanisms that may be necessary.

3.1. IPv4 and IPv6 Architectures

IPv4 was design in 1980 to replace the NCP protocol on the ARPANET. The IPv4 displayed many limitations after two decades [5]. The IPv6 protocol was designed with IPv4's shortcomings in mind. IPv6 is not a superset of the

IPv4 protocol; instead it is a new design. The Internet protocol's design is so vast and cannot be covered fully. The main parts of the architecture relating to security are discussed in detail.

3.1.1. IPv4 Architecture

The protocol contains a couple aspects which caused problems with its use. All these problems do not relate to security. They are mentioned to gain a comprehensive understanding of the Internet protocol and its shortcomings. The causes of problems with the protocol are:

1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

The IPv4 architecture has an address that is 32 bits wide [5]. This limits the maximum number of computers that can be connected to the Internet. The 32 bit address provides for a maximum of two billions computers to be connected to the Internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution.

Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries [5]. Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period of time, but drastic change needs to be made to address this problem. The TCP/IP-based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server [5]. The lack of embedded security within the IPv4 protocol has led to the many attacks seen today.

Mechanisms to secure IPv4 do exist, but there are no requirements for their use [5]. IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication [5]. This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key.

When Internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text-based. As the Internet expanded and technology evolved, other forms of communication began to be transmitted across the Internet. The quality of service for streaming videos and music are much different than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated [5].

3.1.2. IPv6 Architecture

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Security architecture
4. Traffic control

The IPv6 protocol's address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to $3.4 * 10^{38}$ machines. The address bits are used less efficiently in this protocol because it simplifies addressing configuration. The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves.

The security architecture of the IPv6 protocol is of great interest. IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route [5]. The quality of service problem is handled with IPv6. The Internet protocol allows for special handling of certain packets with a higher quality of service. From a high-level view, the major benefits of IPv6 are its scalability and increased security.

3.2. Attacks through the Current Internet Protocol IPv4

There are four main computer security attributes present. These security attributes are confidentiality, integrity, privacy, and availability [6]. Various attack methods relate to these four security attributes. Table 1 shows the attack methods and solutions.

Common attack methods and the security technology will be briefly discussed. Not all of the methods in the table above are discussed. The current technology for dealing with attacks is understood in order to comprehend the current research developments in security.

3.2.1. Common Internet Attack Methods

Common Internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is: when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not so popular like DoS attacks, but they are used in some form.

3.2.1.1. Eavesdropping

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [6].

3.2.1.2. Viruses

Viruses are self-replication programs that use files to infect and propagate [6]. Once a file is opened, the virus will activate within the system.

3.2.1.3. Worms

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [6]. There are two main types of worms, mass-mailing worms and network-aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

3.2.1.4. Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus [6].

3.2.1.5. Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization [7]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

3.2.1.6. IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IPspoofed packets cannot be eliminated [6].

3.2.1.7. Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [7]. Until the handshaking is complete, the system consumes resources. Eventually, the system cannot respond to any more requests rendering it without service.

3.2.2. Technology for Internet Security

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defence and detection mechanisms were developed to deal with these attacks.

3.2.2.1. Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

3.2.2.2. Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [6].

3.2.2.3. Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

3.2.2.4. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware. Anti-Malware tools are used to detect them and cure an infected system.

3.2.2.5. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, between a web browser and the web server, so that any information exchanged is protected within the secured channel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

3.3. Security Issues of IP Protocol IPv6

From a security point of view, IPv6 is a considerable advancement over the IPv4 protocol. Despite the IPv6's great security mechanisms, it still continues to be vulnerable to threats. Some areas of the IPv6 protocol still pose a potential security issue. The new Internet protocol does not protect against mis-configured servers, poorly designed applications, or poorly protected sites. The possible security problems emerge due to the following [3]:

1. Header manipulation issues
2. Flooding issues
3. Mobility issues

Header manipulation issues arise due to the IPsec's embedded functionality which may lead to information attack. The problem is that extension headers need to be processed by all stacks, and this can lead to a long chain of extension headers.

The large number of extension headers can increase the overhead of certain node and is a form of attack if it is deliberate. Spoofing continues to be a security threat on IPv6 protocol. The address space of the IPv6 protocol is large but the protocol is still not invulnerable to this type of attack.

Mobility is a new feature that is incorporated into IPv6. The feature requires special security measures. Network administrators need to be aware of these security needs when using IPv6's mobility feature.

IV. SECURITY IN DIFFERENT NETWORKS

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create "intranets" that are connected to the Internet but protected from it at the same time. Intranet is a private computer network that uses Internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties. There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs).

Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. But for broader data sharing, it might be better to keep the networks open, with these safeguards:

1. Firewalls that detect and report intrusion attempts
2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of email attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates

It was mentioned that if the intranet wanted access to the Internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Figure 2 is a graphical representation of an organization and VPN network.

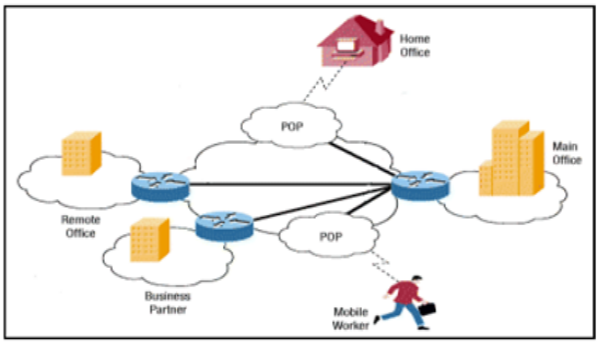

Figure 2: A typical VPN might have a main LAN at corporate office of a company, other LANs are at remote offices and individual users are connecting from out in the field. [8]

V. CURRENT METHODS USED IN NETWORK SECURITY

The network security field is growing by implementation of new features. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assists in understanding current development and projecting the future developments of the field. Hardware developments as well as software development are also active areas in computer security.

5.2. Hardware Developments

The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by entering incorrect password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs.

Smart cards are usually a credit-card-sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure web communications and secure e-mail transactions. It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else. Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they'll be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines.

When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. This PIN was assigned to the user by the administrator at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there's absolutely no danger of it being intercepted. The main benefit is that, the PIN is useless without the smart card, and the smart card is useless without the PIN. There are other security issues of the smart card. The smart card is cost-effective but not as secure as the biometric identification devices.

5.2. Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analysing attack patterns in order to create smarter security software. As the security hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Current research is being performed on security software using neural networks. Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. Research in this area is currently being performed.

VI. RESEARCH PROPOSAL AND FUTURE WORK

The numbers of Internet users are increasing exponentially as compared to the past decades. So, the security issues as well as quality of service have to be improved.

This research proposal is based on two issues:

- Enhancement of Data Security by increasing the level of confidentiality
- Improving the Quality of Service for faster and accurate data transmission

6.1. Enhancement of Data Security

In the past decades the data security are achieved using the private key cryptographic algorithms. To enhance the security level, the public key cryptographic algorithms are introduced. The generalized ring signature method provides a good level of security as well as guarantees for information delivery [9]. The ring signature is based on the clustering of information. In a ring signature, instead of revealing the actual identity of the message signer, it specifies a set of possible signers. The verifier can be convinced that the signature was indeed generated by one of the ring members; however, the verifier is unable to tell which member actually produced the signature. Using a generalized ring signature scheme, a generalized multi-signer ring signature scheme is introduced to increase the level of confidence or enforce cross-organizational joint message signing. Generalized ring signatures algorithm based on RSA algorithm scheme has three advantages and these can be used implemented to increase the level of security. They are:

1. All ring members can share the same prime number p and all operations can be performed in the same domain.
2. By combining with multi-signatures, we can develop the generalized multi-signer ring signature schemes to enforce cross-organizational involvement. It may result in a higher level of confidence or broader coverage on the message source.
3. The proposed ring signature is convertible. It enables the actual message signer will only be capable of generating the ring signature.

Algorithms such as RSA, AES, IDEA uses a single key value. So, the level of security is reduced. Though the RSA algorithm produces a good level of security, still it can be enhanced by addition of the generalized ring signature algorithm.

6.2. Improving the Quality of Service

During the initial stage of networking, information was mostly text-based. As the Internet expanded and technology evolved, other forms of communication began to be transmitted across the Internet. The quality of service for streaming image, audio and videos are much difficult than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated.

ARQ protocol is a data link layer protocol that provides the guarantees that the information will reach the destination. Different types of ARQ protocol can be used for faster and accurate data transmission from source to

destination [10, 11]. The transfer f information can be enhanced by implementing the clustering concept. High impact event represents the information which is frequently used. High impact events are combined to create clusters. The frequently used information is maintained in different clusters such that it can be accessed quickly without involving much searching time. Clustering methods are one of the key steps that lead to the transformation of data to knowledge. Clustering algorithms aims at partitioning an initial set of objects into disjoint groups called clusters such that objects in the same subset are more similar to each other than objects in different groups. Clustering algorithm can be used in metric spaces following *selective Repeat ARQ protocol* having fixed window size for accurate information transmission. The original algorithm was designed to work on data with numerical values. The proposed generalization does not assume anything about the nature of the data, but only considers the distance function over the data set. The efficiency of the proposed approach is demonstrated on *msnbc* data sets. It was proposed using a fixed size data set. But in real life application, the data sets are dynamic in nature. So, the clustering concept has to be implemented using the dynamic data set. The clusters should to be modified automatically as time passes. Since the clusters are frequently updated, the maintenance time will increase significantly. This can be compensated by the reduction in searching time using EHMA. The EHMA (Enhanced Hierarchical Multi Pattern Matching) algorithm [13] will reduce the searching time. Along with EHMA, one way equivalence [15] will increase the level of security to the data. [10, 11] can be used for improving the efficiency by using the group communication techniques. An UPnP controller is implemented to manage devices in the same administrative domain and hence these devices can be treated as members in the same communication group. Using generalized ring signature algorithm, key can be managed for building both point-to-point and broadcast secure channels over the UPnP network [12]. Due to the UPnP feature the energy consumed and bandwidth utilization can be reduced as compared to any traditional approach. The scales of smart living are needed from small to large size applications. As the scale of the space increases, we can expect that the requirements for the two features zero-configuration and secure data communication channels are getting more important. The feature of zero-configuration reduces the cost to setup the network and secure data communication channels guarantee both the privacy and confidentiality of possible sensitive data transmitted in the network. So by integrating these two technologies (UPnP and secure group communication techniques), an almost zero-configuration secure environment can be constructed for smart living spaces. A secure and flexible communication environment is constructed as follows. An UPnP controller is implemented to manage devices in the same administrative domain and hence these devices can be treated as members in the same communication group. Using generalized ring signature algorithm key can be managed for building both point-to-point and broadcast secure channels over the UPnP network. An innovative technique is applied in [14] that works based on the principle of GFGS algorithm. GFGS algorithm deals with the generalized frequent common gram selection for finding the elements which frequently occurs. A 3-tier architecture is proposed in the paper in which the first tire deals with the selection of the generalized frequent common gram selection, second tire deals with the storage of information according to the generalized frequent common gram. The third tire is implemented using SHA-256 algorithm to make the information secure. The information encrypted using SHA-256 is nearly impossible to crack. So, it leads to secured data storage at a faster rate of searching. The security concepts can be implemented for improving the quality of service [16].

VII. CONCLUSION

Network security and QoS is an important field that is increasingly getting attention as the Internet expands. What is going to drive the Internet security most is the enormous and complex set of applications being executed over Internet. The issue of security is similar to an immune system. The immune system fights off attacks and builds itself to fight the security threats. Similarly, the network security will be able to function as an immune system. So, it has to be improved to such level such that information can't be leaked.

Along with the security issues, QoS has to be enhanced for smarter and faster application processing.

REFERENCES

[1] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008

[2] Molva, R., Institut Eurecom, " Internet Security Architecture", in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999

[3] Sotillo S., East Carolina University, " IPv6 security issues ", August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf.

[4] "Improving Security," http://www.cert.org/tech_tips, 2006.

[5] J., "IPv6: the next internet protocol", April 2005, www.usenix.com /publications /login / 2005-04/pdfs/ andress0504.pdf.

[6] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

[7] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[8] Tyson, J., "How Virtual private networks work," http://www.howstuffworks.com/vpn.htm .

[9] Jian Ren, Member, IEEE, and Lein Harn: Generalized Ring Signatures, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 5, NO. 3, JULY-SEPTEMBER 2008.

[10] P. C. Sethi, C. Dash: High Impact Event Processing using Incremental Clustering in Unsupervised Feature Space through Genetic algorithm by Selective Repeat ARQ protocol: ICCCT- 2nd IEEE Conference – 2011, pp. 310-315.

[11] Atul Kamble, Incremental Clustering in Data Miningusing Genetic Algorithm, International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010. 1793-8201.

[12] P. C. Sethi: "UPnP and Secure Group communication Technique for Zero-configuration Environment construction using Incremental Clustering", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278 – 0181, Vol. 02 Issue 12, December – 2013.

[13] Tzu-Fang Sheu, Nen-Fu Huang, and Hsiao-Ping Lee, "In-Depth Packet Inspection Using a Hierarchical Pattern Matching Algorithm", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 2, APRIL-JUNE 2010, Page175-188

[14] P. C. Sethi, P.K. Behera, "Secure Packet Inspection using Hierarchical Pattern matching implemented Using Incremental Clustering Algorithm", December-22-24, ICHPCA-2014 (IEEE International Conference)

[15] Kaoru Kurosawa, *Member, IEEE*, and Tsuyoshi Takagi, "One-Wayness Equivalent to General Factoring", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 55, NO. 9, SEPTEMBER 2009, Page 4249 - 4262

[16] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret, Advances in Cryptology", ASIACRYPT, 2001

Table1: Attack Methods and Security Technology [6]

Computer Security attributes	**Attack Methods**	**Technology for Internet Security**
Confidentiality	Eavesdropping, Hacking, Phishing, DoS and IP Spoofing	IDS, Firewll, Cryptographic Systems, IPSec and SSL
Integrity	Virus, 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 Boot Recording Infectors	IDS, Anti-Malware Software and Firewall

Purna Chandra Sethi received the B. Tech and M.Tech degrees in Information Technology Engineering and Computer Science Engineering from College of Engineering & Technology, Bhubaneswar. He has qualified UGC-NET three times in Computer Science and Applications. He is currently pursuing PhD in Department of Computer Science at Utkal University, Odisha, India. His current research area of interest is Network Security and QoS. He is a life time member of CSI, ISTE, IAENG, CSTA.

Dr. P. K. Behera is currently working as Reader at Department of Computer Science, Utkal University, Bhubaneswar, Odisha, India. He has more than two decades of teaching experience. His area of interest is MANET, Wireless Network, Distributed Systems, Mobile Computing, Network and Information Security, Software Engineering. He has published number of research papers in reputed International Conferences and Journals. He is a reviewer of many national and International referred Journals. He is the Secretary of CSI Bhubaneswar Chapter.

