A Study of the Novel Approaches Used in Intrusion Detection and Prevention Systems

Usman Asghar Sandhu, Sajjad Haider, Salman Naseer, and Obaid Ullah Ateeb

***Abstract*—Security is an important and serious issue for every type of network. Many network environments specially those where computers are used as nodes are prone to an increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the computer systems, servers and communication channels. Though Firewalls are used as a necessary security measure in a network environment but still different types of security issues keep on arising. In order to further strengthen the network from intruders, the concept of intrusion detection system (IDS) and intrusion prevention system (IPS) is gaining popularity. IDS is a process of monitoring the events occurring in a computer system or network and analyzing them for sign of possible incident which are violations or imminent threats of violations of computer security policies or standard security policies. intrusion prevention system (IPS) is a process of performing intrusion detection and attempting to stop detected possible incidents. This study aims to identify different types of Intrusion Detection and Prevention techniques discussed in the literature.**

***Index Terms*—Anomaly, detection, intrusion, prevention, signature.**

I. Introduction

Due to the widespread usage and deployment of networks their survivability and security is one of the most important and challenging task. An organization without network is like a vehicle without fuel and making sure those organizations network remains up all the time without any disruptions is the responsibility of the persons deputed for this task. Only the smooth network connectivity can ensure that clients will use it for communication (e.g. chat, email, audio and video conversation), online shopping, debit and credit card details and exchange of personal information etc. Due to the rapid growth in the technology and widespread use of the Internet, a lot of problems have been faced to secure the system's critical information within or across the networks because there are millions of people attempting to attack on systems to extract confidential and critical information. A huge number of attacks have been observed in the last few years. Intrusion detection and prevention systems (IDPS) play an immense role against those attacks by protecting the system's critical information. As firewalls and anti viruses are not enough to provide full protection to the system, organizations have to implement the Intrusion Detection and Prevention Systems (IDPS) to protect their critical information against various types of attacks.

Manuscript received November 23, 2011; revised December 10, 2011.

U. A. Sandhu is with Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad Campus (e-mail: usmanasghar001@yahoo.com).

S. Haider is with the Department of National University of Modern Languages (NUML), Islamabad, Pakistan (e-mail: sajjadhyder@hotmail.com).

II. Intrusion Detection System (IDS)

Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects intrusive behavior. Intrusion detection system (IDS) monitors network traffic and its suspicious behavior against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions. An IDS is a set of techniques and methods that are used to detect suspicious activities both at the network and host level. There are two main types of intrusion detection system (IDS), host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS).

III. Intrusion Prevention System (IPS)

IPS is an advance combination of IDS, personal firewalls and anti-viruses. The purpose of an intrusion prevention system (IPS) is not only to detect an attack that is trying to interrupt, but also to stop it by responding automatically such as logging off the user, shutting down the system, stopping the process and disabling the connection etc. Similar to IDS, IPS can be divided into two types, i.e. host-based intrusion prevention systems (HIPS) and network-based intrusion prevention systems (NIPS) [1].

IV. Types of Intrusion Detection Systems

There are two main types of intrusion detection systems.

A. Anomaly Detection

Anomaly detection technique store the systems normal behavior such as kernel information, system logs event, network packet information, software running information, operating system information etc into the database. If any abnormal behavior or intrusive activity occurs in the computer system which deviates from system normal behavior then an alarm is generated. Anomalous activities that are not intrusive are flagged as intrusive. This will result in false-positive, i.e. false alarm. Intrusive activities that are not anomalous result in false negative [2].

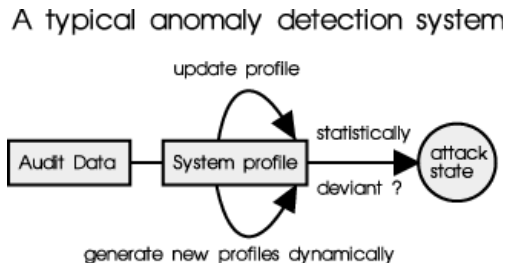

Fig. 1. Anomaly detection [3]

B. Signature Detection

The concept behind signature detection or misuse detection scheme is that it stores the sequence of pattern, signature of attack or intrusion etc into the database. When an attacker tries to attack or when intrusion occurs then IDS matches the signatures of intrusion with the predefined signature that are already stored in database. On successful match the system generates alarm.

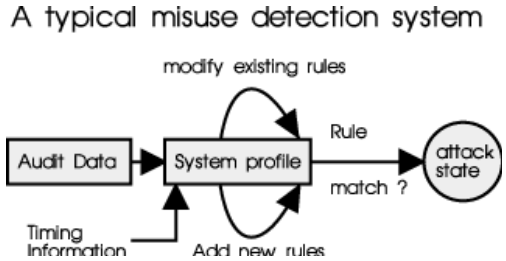

Fig. 2. Signature detection [3]

V. Intrusion Detection and Prevention Systems

IDPS is a process of monitoring the events occurring in a computer system or network and analyzing them for possible incidents, which are violations or imminent threats of violations of computer security policies, acceptable use of policies or standard security practices and process of performing ID and attempting to stop detected possible incidents.

Following are the types of Intrusion Detection and Prevention Systems.

A. Host-Based Intrusion Detection and Prevention System

If we merge both IDS and IPS on a single host then it is known as a host-based intrusion detection and prevention system (HIDPS). host-based intrusion detection and prevention system (HIDPS) relates to processing data that originates on computers themselves, such as event and kernel logs. HIDPS can also monitor that which program accesses which resources and might be flagged. HIDPS also monitors the state of the system and makes sure that everything makes sense, which is basically a concept of anomaly filters. HIDPS normally maintains a database of system objects and also stores the system's normal and abnormal behavior. The database contains important information about system files, behavior and objects such as attributes, modification time, size, etc. If any suspicious or anomaly behavior occurs then it generates an alarm and takes some appropriate response against detected threat or attack.

B. Network-Based Intrusion Detection and Prevention System

Intrusion detection is network-based when the system is used to analyze network packets. Network-Based intrusion detection and prevention system (NIDPS) capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviors. Several sensors are used to sniff the packets on network which are basically computer systems designed to monitor the network traffic. If any suspicious or anomaly behavior occurs then they trigger an alarm and pass the message to the central computer system or administrator (which monitors the IDPS) then an automatic response is generated. There are further two types of NIDPS. Promiscuous-mode network intrusion detection is the standard technique that "sniffs" all the packets on a network segment to analyze the behavior. In Promiscuous-mode Intrusion detection systems, only one sensor is placed on each segment in the network. Network-node intrusion detection system sniffs the packets that are bound for a particular destination computer. Network-node systems are designed to work in a distributed environment [4].

VI. Literature Review

The aim of this paper [5] is to address the issues of information security because most of the organizations are depending on the internet to communicate with the people or with the systems to provide them news, online shopping, email, credit card detail and personal information. This paper [5] describes the security needs of an organization to protect their critical information from attacks. A well trained staff and analyst are required to continuously monitoring the system. Still a huge effort is required to construct new security strategies which are discussed in [6], [7], [8].

Reference [6] Provides a multilayer approach in IDS to monitor a single host. Multilayer approach [6] consists of three layers. File analyzer monitors the particular files and folders on the host system that could be under attack by intruders. This layer creates the signatures and threshold values created by the user into the database. System Recovery sends those signatures and threshold values into the database. Connection analyzer creates the signature of the other computer specified by the user for blocking. The advantage of this technique is that it provides both signatures based and anomaly based detection and protects the system against harmful attacks. Multilayer approach [6] in IDS requires a large amount of memory to store the data of the system and network traffic. IDS should have to continuously update the system whenever it detects any intrusion.

Proventia desktop is a software based solution [9] which protects the system from network layer up to application layer by known and unknown attacks. Proventia desktop analyze the packets on network or on the single host system. Once it checks all the packets that they are not malicious then will execute in live environment. If any suspicious or anomaly behavior occurs it will stop it by alert and will show the message to allow execute or terminate the file. This uses both signature and anomaly detection to protect the system by

analyzing the network traffic. This software has great flexibility to set different type of filtering rules. We do not have a single silver bullet to stop everything. Any single technology represents a single point of failure. The major draw of HIPS is high rate of false-positive. A lot of time and trained staff is required to monitor the IDPS [9].

TABLE I: CRITICAL ANALYSIS

IDPS	HIDPS and NIDPS	Operating system and Application level approach	Yes	Yes	Yes	Yes	Signature based and anomaly based	Automatic response, reduce human effort	Cost ineffective, implementation, updating, monitoring issues
IDPS	HIDPS	OS and Application level approach	Yes	Yes	Yes	Yes	Signature based and anomaly based	Strong detection and protection mechanism	A large amount of memory is requires
IDPS (Proventia Desktop)	HIDPS and NIDPS	Network layer to application layer level	Yes	Yes	Yes	Yes	Signature based and anomaly based	Flexibility of customize, Cost effective	High rate of false-positive, well trained analysts are required
IDPS	HIDPS and NIDPS	In-source and out-source	Yes	Yes	Yes	Yes	Signature based and anomaly based	Secured infrastructure	Well trained analysts are required
IDPS (SNORT)	NIDPS	OS and Application level approach	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion
IDPS	HIDPS	Secure mobile agent	Yes	Yes	Yes	Yes	Signature based and anomaly based	Real time response, reduce human effort	Security of mobile agent, needs to adopt some other techniques
IDS (PH)	HIDS	sequence matching, inserting malicious sequence and no-op	Yes	No	Yes	No	Signature and anomaly based	Modeling or analysis of different attacks and their techniques	Not fully secured, still have huge risk of attack.
IDPS	HIDPS and NIDPS	Sequence matching , malicious matching	Yes	Yes	No	No	Signature based	Automated response to malicious attacks	Unable to detect and respond to anomaly behavior
IDS	HIDS and NIDS	String matching	Yes	No	No	No	Signature based	Efficient and Faster	Memory and implementation issues
IDS	NIDS	Sequence matching, distributed env.	Yes	No	No	No	Signature based	Flexibility of self configuration	Large amount of memory and training staff is required
IDS	HIDS and NIDS	Data mining, data fusion	Yes	Yes	No	No	Signature based and anomaly based	Centralized architecture	No mechanism of protection
IDS	HIDS	Decision tree, statistical approach	Yes	No	Yes	No	Signature based and anomaly based	Less false positive, Efficient detection	No mechanism of protection
IDPS	HIDPS and NIDPS	Peer to peer	Yes	Yes	Yes	Yes	Signature based and anomaly based	Reliable trusted and efficient	Memory and Implementation issue
IDS	HIDS	Virtual machine	Yes	No	No	No	Signature based	Cost effective, Efficient	Unable to detect anomaly behavior
IDPS	NIDPS	SNORT, tripware, mysql	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion

This paper [10] helps an organization to take an informal decision in order to select the IDS. This model divides the IDS into two types, in-source and out-source. The term in-source or in-house represent to an organization's

employees who directly operate the IDS. The term out-source refers to the management security services provider (MSSP) who has contract with the organization for performing IDS services such as monitoring, configuring and updating on both host based and network based systems. Provide a security to an organization against attacks is a key business of MSSP [10]. MSSP spend most of the time to examine new technology to secure an organization better than before.

According to [11], Snort and source fire are best IPSs for a multinational company. SNORT is IPS tool, based on signature technique that detects the suspicious behavior of attack and generate an automate respond to a possible detected attack in real time. Source fire is used to define the limitation of Snort. This product provides high flexibility that allow to the user to self configure and modify its source code. The major drawback of Snort is that it use only signature based technique to detect the intrusion but if an abnormal or anomaly behavior occur then it will not possible for SNORT to detect that anomaly attack [11].

This paper [12] provides a technique of secure mobile agent in IDPS for the security of system. Secure mobile agent monitor the system, process the logs, detect the anomaly or attacks, protect the host by automate real time response and perform security management. The advantages of [12] secure mobile agent are: accurate event monitoring filtering the systems logs and intelligent response in real time against illegal, abnormal and unauthorized events. Major disadvantage of this technique is that the IDPS is still needs to adopt some security infrastructures for the protection of mobile agent because if the target of the attackers is mobile agent then it will be difficult to protect the system to being hacked [12].

David and Paolo examine [13] many hose based anomaly intrusion detection system and briefly describe attacks security to evasion attacks. This technique based on that how application interacts with the operating system, sequence matching, inserting malicious sequence and inserting no-op. This paper mainly focused on exploring the techniques of several attacks to break the security of IDS and prove it by giving the example of an attack on IDS and defense against that particular attack. There experiments shows that many attacks can break IDS without detection. The example discussed in [13] consist only method on a single operating system using particular IDS(PH). But there is a huge risk for other operating system and other implemented IDS. This technique is unaware about that how much effort and knowledge is required to produce such an attack and also unaware about that how attackers can predict that how IDS actually works.

Harley [4] defines the difference between host based and network based intrusion detection and prevention system that is already discussed above. This paper describes two types of network intrusion detection system: promiscuous-mode and network-node. Harley mainly focused on the automated response by the IDS to stop attackers or intruders while attacking by logging off the user, shutdown the system, stop the process and disable the connection. The main disadvantage is that this IDS only respond to the signature based detected attacks but not to the anomaly based detected attacks. So there is still a need of human interaction who took real time action to resolve issue [4].

Novel string matching technique [7] is an optimization of other matching algorithms. Novel string matching algorithm break the string into small sets of state machines. Each state machine recognizes the subset of string. If any suspicious behavior occurs then the system broadcast the information about intruder to every module (state machine) which holds the database in order to defined rules. They compare the signatures of intruder with predefined detected signatures sends information back to the system which then respond to attack. Novel string matching algorithm is most efficient and ten times faster than the other existing systems and it consumes less resources. The major issue with this string matching algorithm is its practical implementation and it requires a large amount of memory. This algorithm is not capable to detect the anomaly behavior of the intrusion as [13], [14].

According to S. Mrdović and E. Zajko [15], distributed IDS is used to analyze the system in which multiple sensors are placed in selected network segments that observe the network traffic behavior. SNORT is used as an analysis engine. Mysql is used to log the events with the help of SNORT. Distributed IDS is managed by management console which monitors and configures the IDS. This IDS provides a greater protection against attacks because multiple computers are continuously monitoring and preventing the network from malicious attacks [16]. Large memory and well trained security analysts are required to implement and continuous management of the system [16].

This paper [2] describes the security of IDS. It highlights two different techniques of IDS. Misuse detection and anomaly detection. Three different approaches data mining, data fusion and immunological based approach used in IDS. This paper provides brief information about existing intrusion detection technology. It evaluates the challenges and future directions of intrusion detection technology. The approaches that are discussed in [10], [7] and [14] are much sufficient for IDPS to detect and respond to anomalies in real time. The techniques that are discussed in [2] are facing the lack of high speed to detect or respond to the intrusion in real time.

This paper [8] proposed intrusion detection techniques by combining multiple hosts in order to detect multiple intrusions and to reduce false-positive rate. Hidden Markov Model (HMM) is a speech recognition technique that is used for modeling the system call events. Statistical technique gives the percentage of resource usages and system call events. Decision tree is used to model or classify the type intrusion to examine the future challenges. This technique [8] has advantage of less false-positive rate that increases performance of detection. If this IDS adopts the mechanism of protection that is discussed in [10] and [4] then the system can be secured in a better way.

Indra (intrusion detection and rapid action) [16] provides a tool that uses peer to peer approach for the security of network. This technique works in a distributed environment by distributing the intruder's information on peer to peer network. If Indra finds any interrupt then it generates an alert to the central authority which then reacts to the intruder by disconnecting the services or disable internet connection.

Indra is reliable and trusted. Efficient communication is occurred in trusted peer to peer network. It has strong polices of inspection and reaction against attacks. The drawback of Indra is its implementation issue. It requires a large amount of memory to store all the collected information about intruder. But still this tool does not provide enough and strongest security to an organization as the technique discussed in [6], [9].

This paper [14] proposed architecture to protect host-based intrusion system through virtual machine. The main idea of this technique is to observe the system behavior or monitor the system inside and virtual machine which then monitor by the host. Detection and response mechanism are operating in host that is outside the virtual machine and out of range from intruder. The benefits of virtual machine are: efficient, duplication of real operating system, invisible and inaccessible to intruders. Multiple virtual machines can runs simultaneously on a same hardware. The major benefit is cost effectiveness then other techniques discussed in [6], [9].

Matt and Andrew in [1] Investigates the IDPS and also IDS/IPS tools. They mainly focus on NIDS. They evaluate that IPS is an evolved version of IDS and use SNORT to detect malicious behavior. SNORT is a NID tool that is use to configure the log into the database directly. My SQL installed to creating the schema and configure the setting of permissions. TRIPWIRE software is used to monitor the changes in specific files and enable the SNORT to continuously check logs. The major benefit of SNORT is that it can detect the large number of different attacks such as viruses, Denial of services, malware and many more [1]. It provides signature based technique to detect intrusion. The drawback of SNORT is that it only detects the signature base technique. If an anomaly behavior occur then this technique is useless.

This paper [17] provides an experimental study of IDPS SNORT using which consists on a virtual network infrastructure that is installed and configured on a computer system. The objective of this paper is to provide the comprehensive study to detect the malicious arracks and real time response. First install multiple virtual machines on a single computer system by using VMware work station 6.0. There will be at least three virtual machines that will provide the functionality of victim host, normal host, attack host and detection host. The detection host is responsible to monitor malicious activity on network segment. The attack host is responsible to launch the attack against victim host. The Linux CentOS will act as detection host which is used to generate normal and abnormal traffic. The Window XP will generate normal traffic and act as victim host.

In order to examine how attacker finds vulnerabilities in network or computer system. Different tools are used to find vulnerabilities and exploit an attack. Metasploit is used to launch DOS attack or buffer over flow attack. Nmap is used to get the information about victim computer to find vulnerabilities. A lot of tools provide knowledge about how an attacker exploits computer system by using vulnerabilities e.g., Angry IP Scanner, UDPFlood, Backtrack, and hydra.
After getting all the information about attacks the next step is to analyze the signature of attack e.g., characteristics of backdoor attacks, how Dos attack works, Buffer overflow cause, Scanning etc.

This analysis helps to built SNORT IDPS rules. SNORT is an open source IDPS tool used to detect the known attacks. The goal of IDPS is to make sure that network traffic is attack or normal traffic. Now collect the computer normal activities by downloading and uploading and uploading file and save it in trace file then combine this normal traffic with the attacked traffic and store it an SNORT database.

By storing this large amount of traffic we can check the performance of SNORT and evaluate that it can effectively detect the intrusion or not. Tcpreplay is a tool which is used to replay the previous captured traffic to analyze the alert of intrusion detected by the SNORT [17].

VII. Conclusion and Future Work

Different techniques are discussed in this paper to support the security of an organization against threats or attacks. On the other side attackers are discovering new techniques and ways to break these security policies. Firewalls, antivirus and antispyware are limited to provide security to the system against threats. The only way to beat them is to know about their techniques that they use for attack. So, security organizations will have to adopt such a strongest model or mechanism which provides strongest protection against threats to ensure that the system will remain secure. IDPS provides the facility to detect and prevent from attacks by inheriting multiple approaches like secure mobile agent, virtual machine; high throughput string matching, multilayer and distributed approach provide greater and strongest security against multiple attacks. There are still many ways to improve the virtual machine based intrusion detection and prevention system and in future we will propose a solution to further secure virtual machine based implementation.

Acknowledgement

We would like thank Dr. Mureed Hussain and Dr. Naveed Riaz Ansari for their valuable comments and suggestions for the improvement of this paper. Similarly we are also thankful to the SZABIST Islamabad Campus Network support team for the support of necessary Hardware/Software required to carry out this researc.

References

[1] M. Carlson and A. Scharlott, "Intrusion detection and prevention systems," 2006.

[2] Y. Bai and H. Kobayashi, "Intrusion detection systems : technology and development," presented at 17th International Conference of Advanced Information Networking and Applications, 27-29 March, 2003.

[3] A. Sundaram "An Introduction to Intrusion Detecion," 1996.

[4] H. Kozushko "Intrusion detection: host-based and network-based intrusion detection systems", *Independent Study*, September 11, 2003.

[5] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Information Management and Computer Security Journal*, vol. 18, no: 4, pp. 277-290, 2010.

[6] O. Awodele, S. Idowu, O. Anjorin, and V. J. Joshua, "A multi-layered approach to the design of intelligent intrusion detection and prevention system (IIDPS)," vol. 6, Babcock University, 2009.

[7] L. Tan and T. Sherwood, "A high throughput string matching architecture for intrusion detection and prevention, " *in Proceedings of the 32nd annual international symposium on Computer Architecture*, IEEE Computer Society Washington, DC, USA 2005.

[8] S. Han and S. Cho, "Combining multiple host-based detectors using decision tree," presented at Australian Joint Artificial Intelligence Conference, 2003.
[9] J. Chee, "Host intrusion prevention systems and beyond," *SANS Institute*, June 2, 2008.
[10] V. Fitzparick, "Intrusion Detection and Prevention In-sourced or Out-sourced," *SANS Institute*, July 8, 2008.
[11] M. Guimaraes and M. Murray "Overview of Intrusion Detection and Intrusion Prevention," in *Proceedings of the 5th annual conference on Information security curriculum development,* ISBN: 978-1-60558-333-4, New York, USA, 2008.
[12] A. Shibli and S. Muftic, "Intrusion Detection and Prevention System using Secure Mobile Agents," *IEEE International Conference on Security and Cryptography*, pp. 76-82, Porto Portugal, July, 2008.
[13] D. Wagner and P. Soto "Mimicry Attacks on Host Based Intrusion Detection Systems," *9th ACM Conference on Computer and Communications Security*, Washington, DC, November 18–22, 2002.
[14] M. Laureano, C. Maziero1, and E. Jamhour "Protecting Host-Based Intrusion Detectors through Virtual Machines," *The International Journal of Computer and Telecommunications Networking*, May, 2007.
[15] S. Mrdovic and E. Zajko "Secured Intrusion Detection System Infrastructure," *University of Sarajevo / Faculty of Electrical Engineering*, Sarajevo, Bosnia and Herzegovina, 2005).
[16] R. Janakiraman and Q. Zhang "Indra: A peer-to-peer approach to network intrusion detection and prevention," *Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2003.
[17] T.-S. Chou "Development of an Intrusion Detection and Prevention Course Project using Virtualization Technology," *International Journal of Education and Development using Information and Communication Technology* (IJEDICT) 2011.

Usman Asghar Sandhu completed his BS Honors in Computer Science from University of the Punjab, Gujranwala Campus, (PUGC) Pakistan in 2010. Currently he is a student of MS(CS) leading to PhD with specialization in Network Security from Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, (SZABIST) Islamabad Campus, Pakistan.

Sajjad Haider is Assistant Professor at the Department of Information Technology in National University of Modern Languages (NUML), Islamabad, Pakistan. He holds Bachelors and Masters Degrees in Computer Science and is a PhD Scholar in Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad Campus. Before joining NUML in 2002, he was working as Network Manager in National Institute of Electronics (NIE), a Research and Development Organization working under the Ministry of Science and Technology, Government of Pakistan.

Sajjad's research interests lie mainly in the area Parallel and Distributed Computing, High Performance Computing, Fault Tolerant Computing and Network Security. He has many publications in National and International Conferences and in refereed Journals. He is also the paper reviewer of many International Conferences and is a member of IACSIT.

Salman Naseer Completed his M.Sc. Computer Science from University of the Punjab Lahore Pakistan in 2004. He is currently pursuing MS leading to PhD in Computer Science (Specialization in Computer Networks) from Comsats Institute of Information Technology (CIIT) Lahore, Pakistan. He is working as a Lecturer in the Department of Information Technology, University of the Punjab, Gujranwala Campus.

Obaid ullah Ateeb Bhatti Completed his BS(CS) Hons. from University of the Central Punjab in 2005 and MIT from University of the Punjab in 2007. He is doing MS leading to PhD in Computer Science (Specialization in Computer Networks) from Comsats Institute of Information Technology (CIIT) Lahore, Pakistan. Currently he is working as a Lecturer in Department of Information Technology, University of the Punjab, Gujranwala Campus.