Distributed Cloud Intrusion Detection Model

Irfan Gul, M. Hussain

SZABIST Islamabad, Pakistan
E-mail: irfan24br@gmail.com, hmureed@yahoo.com

Abstract

Intrusion prospects in cloud paradigm are many and with high gains, may it be a bad user or a competitor of cloud client. Distributed model makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDOS) and Cross Site Scripting (XSS). Confronting new implementation situations, traditional IDSs are not well suited for cloud environment. To handle large scale network access traffic and administrative control of data and application in cloud, a new multi-threaded distributed cloud IDS model has been proposed. Our proposed cloud IDS handles large flow of data packets, analyze them and generate reports efficiently. Transparent reports are instantly send for information of cloud user and expert advice for cloud service provider's network mis-configurations through a third party IDS monitoring and advisory service.

Keywords: *NIDS, HIDS, DOS, DDOS, Cloud IDS*

1. Introduction

Cloud computing has revolutionized the IT world with its services provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability. Cloud computing has three basic abstraction layers i.e system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications) [1]. Hardware layer is not included as it does not directly offer to users. Cloud computing also has three service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates users by providing platform on which applications can be developed and run. IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. SaaS model makes user worry free of installing and running software services on its own machines. Presently, Salesforce.com, Google and Amazon are the leading cloud service providers who extend their services for storage, application and computation on pay as per use basis. Since Cloud computing supports distributed service oriented paradigm, multi-domain and multi-users administrative infrastructure, it is more prone to security threats and vulnerabilities. Currently the biggest hurdle in cloud adoption by most of the corporate organizations is its security. Due to its distributed nature, cloud environment has high intrusion prospects and suspect of security infringements. Large business organizations place there data into Cloud and get worry-free as a Cloud service provider (CSP), stores & maintains data, application or infrastructure of cloud user. Relinquishing the control over data and application poses the challenges of security like data integrity, confidentiality and availability.

Data, application and services non-availability can be imposed through Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and both cloud service provider and users become handicap to provide or receive cloud services [2]. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism.

IDSs are host-based, network-based and distributed IDSs. Host based IDS (HIDS) monitors specific host machines, network-based IDS (NIDS) identifies intrusions on key network points and distributed IDS (DIDS) operates both on host as well as network.

IDSs produce alerts for the administrators which are based on true positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system. Efficiency of IDS can be judged by its high detection rate and a low false positive rate [3]. IDS can be compared with fortress defense against any intrusion whereas firewall can act as a first line of defense against the outbound attackers. Firewalls can be by passed through stealth attacks strategies with the help of e-mail based Trojan horse viruses by a concealed access through DNS or ICMP protocols [4].

IDSs can detect intrusion patterns by critically inspecting the network packets, applying signatures (pre-defined rules) and generating alarms for system administrators. IDS uses two method of detection i.e anomaly detection, that works on user behavior patterns and suspicious behavior. Other method is misuse detection that can detect through renowned attack patterns and matching a set of defined rules or attack against system vulnerabilities through port scanning [5].

In Cloud computing, where massive amount of data is generated due to high network access rate, IDS must be robust against noise data & false positives. Since Cloud infrastructure has enormous network traffic the traditional IDSs are not efficient enough to handle such a large data flow. Most known IDSs are single threaded and due to rich dataset flow, there is a need of multi-threaded IDS in Cloud computing environment.

In a traditional network, IDS monitors, detects and alert the administrative user for network traffic by deploying IDS on key network choke points on user site. But in Cloud network IDS has to be placed at Cloud server site and entirely administered and managed by the service provider. In this scenario, if an attacker manages to penetrate and damage or steal user’s data, the cloud user will not be notified directly. The intrusion data would only be communicated through the service provider and user has to rely on him. The cloud service provider may not like to inform the user about the loss and can hide the information for the sake of his image and repute. In such a case, a neutral third party monitoring service can ensure adequate monitoring and alerting for cloud user.

In this paper, we have proposed an efficient multi-threaded cloud IDS, administered and monitored by a third party ID monitoring service, who can provide alert reports to cloud user and expert advice for cloud service provider. In order to resolve the issues which traditional IDSs can not resolve, an efficient and reliable distributed Cloud IDS model is proposed.

The remaining part of the paper is organized as follows. The section II discusses the security concerns and issues in the area of Cloud computing. Section III deals with the related work in the field of cloud IDS. In section IV, we carried out analysis of traditional and cloud IDS. In the next section, the proposed model is described to show how specific features of the distributed Cloud IDS can increase the efficiency of the system and decrease the network load by using multi-threaded approach. Moreover, transparency of information can be achieved through a third party IDS monitoring service. Advantages of proposed model are discussed in section VI. We have tested our approach and measured the efficiency of proposed model in section VII. Finally, we give conclusion and future work in sections VIII and IX, respectively.

2. Security Issues in Cloud Computing

Cloud computing has emerged as a promising IT services provisioning paradigm, but its security issues are impending its widespread adoption [6]. Security threats can be categorized as follow:

2.1. Network and host based attacks on remote Server

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

2.2. Cloud security auditing

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

2.3. Sub-contracting cloud services

Cloud user makes a contract or agreement for service provisioning with the cloud service provider. Subcontracting of cloud services by cloud service provider to another service provider poses security issues like non-repudiation or not owing the responsibility, if something goes wrong with precious data and application of cloud user.

2.4. Non-availability of cloud services

Non-availability of services due to Cloud outages can cause monetary loss to cloud user organization. A deliberate and comprehensive Service Level Agreement (SLA) must be written among user and provider covering all the relevant legal and service provisioning issues and details.

2.5. Lack of data interoperability standards

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user’s data and application may not be compatible with other vendor’s data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider.

2.6. Cloud data confidentiality issue

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service provider’s end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case.

Above mentioned cloud security issues are a few and dynamicity of cloud architecture are facing new challenges with rapid implementation of new service paradigm.

3. Related Works

3.1. Intrusion detection for grid and cloud computing

Cloud and Grid computing are the most vulnerable targets for intruders' attacks due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host based IDSs (HIDS) are not able to find the hidden attack trail. Kleber, schulter et al. [7] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent user actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion.

The authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud users.

3.2. Intrusion detection in the cloud

Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach. In cloud computing, user data and application is hosted on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS should be the user and not the provider of cloud services. In this paper [1], Roschke and Cheng et al. have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to 'Event Gatherer' program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.

3.3. Integrating a network IDS into an open source cloud computing environment

Security concerns in cloud computing are the main hurdles in cloud adoption. To deny use of services hosted by a cloud service provider, denial of service (DOS) or distributed denial of service (DDOS) attacks are used by the offender. Traditional IDSs need a special consideration for a dynamic and complex cloud environment. Network based IDSs are more appropriate for cloud infrastructure due to the advantage of monitoring the host virtual machine infrastructure without being compromised. Whereas in HIDS if host is compromised the intrusion detection system monitoring would be neutralized and could jeopardize the security of whole system. Claudio et al. have proposed [8] to emplace a NIDS on virtual switch of the physical machine hosting virtual machines of clients using open source 'Eucalyptus' cloud computing framework. The Eucalyptus based cloud IDS would be able to observe all in-bound and out-bound traffic from the entry point of traffic. The proposed idea is based on installation of IDS on each physical machine hosting other client virtual machines rather to deploy IDS on a single point. The suggested solution could proved to be effective and efficient in terms of load sharing of large volume of data, no packet loss and low computational consumption. The authors have validated their idea through experiment and found that IDS hosted at a single point consumes more CPU load than IDS placed at various physical machines and consuming local resources. Also in case if single IDS is compromised by the offender, it would not affect the working of other IDSs and they still be operating properly.

4. Traditional IDS vs Cloud IDS

4.1. Traditional HIDS and NIDS Weaknesses

Traditional IDSs are not suitable for a dynamic and distributed cloud environment. Network based IDSs (NIDS) have the limitation that they could not detect encrypted data traffic. Also host based IDSs (HIDS) are not well suited to find the concealed attack records.

4.2. NIDS and HIDS attack resistance

NIDS gives better observation and more resistibility against offending attacks, but lacks the knowledge about host system. On the other hand, HIDS provides security against the host system but still could not detect and resist attacks on other hosts or network and are vulnerable to evasion attacks.

4.3. Multi-threaded IDS for cloud

Most known IDSs are single threaded whereas due to colossal amount of traffic and data flow there is a need of multi-threaded IDS in Cloud computing environment.

4.4. Integrated IDS solution for cloud

The distributed nature of Cloud infrastructure and its service oriented paradigm it is highly vulnerable to multifarious network and host security attacks. A single IDS rule sets/ signature may not be sufficient for such a diverse nature of malicious attacks. Therefore, Cloud IDS requires an integrated solution incorporating renowned IDS sensors to communicate over a single platform. An integrated IDS solution would cover all known attacks signatures as well as knowledge of new threats.

4.5. Optimized IDS techniques for cloud

With the advent of internet, intrusion attacks have gained sophistication over the time. In the beginning, attackers need to have a proficient knowledge of computer network system. But gradually with the induction of sophisticated hacking tools a novice attacker could infiltrate and damage a system. Figure 1 [4], shows a graphical view of this scenario. Distributed and sophisticated attacks could not be detected by the present available intrusion detection systems. Researchers have suggested various intrusion detection techniques basing on knowledge and behavior based techniques. These techniques could be employed to have an optimized IDS solution for complex future attacks detection.

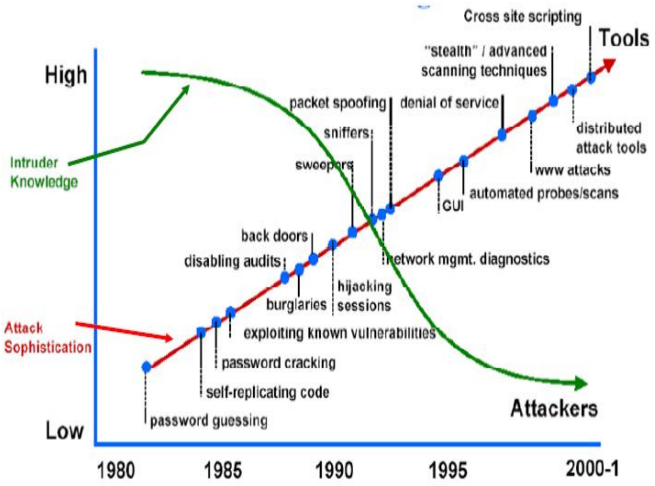

Figure 1. Intruder’s Technical Knowledge Against Sophistication of Attacks and Tools [4]

5. Proposed Model

Our proposed model is an efficient and effective distributed Cloud IDS which uses multi-threading technique to improve IDS performance over the Cloud infrastructure. Our multi-threaded IDS is a NIDS that uses sensors to sensitize and monitors network traffic as well as check for malicious packets. The system then sends intrusion alarms to a third party monitoring service, which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider.

Cloud computing provides application and storage services on remote servers. The clients do not have to worry about its maintenance and software or hardware up-gradations. Cloud model works on the ‘concept of virtualization’ of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine. Deploying HIDS in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the rapid flow of high volume of data as in cloud model, there would be issues of performance like overloading of VM hosting IDS and dropping of data packets. Also if host is compromised by an offending attack the HIDS employed on that host would be neutralized. In such a scenario, a network based IDS would be more suitable for deployment in cloud like infrastructure. NIDS would be placed outside the VM servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. Such NIDS would still be facing the issue of large amount of data through network access rate in cloud environment. To handle a large number of data packets flow in such an environment a multi-threaded IDS approach has been proposed in this paper. The multi-threaded IDS would be able to process large amount of data and could reduce the packet loss. After an efficient processing the proposed IDS would pass the monitored alerts to a third party monitoring service, who would in turn directly inform the cloud user about their system under attack. The third party monitoring service would also provide expert advice to cloud service provider for mis-configurations and intrusion loop holes in the system. Figure 2, shows the proposed IDS model. The cloud user accesses its data on remote servers at service provider's site over the cloud network. User requests and actions are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider.

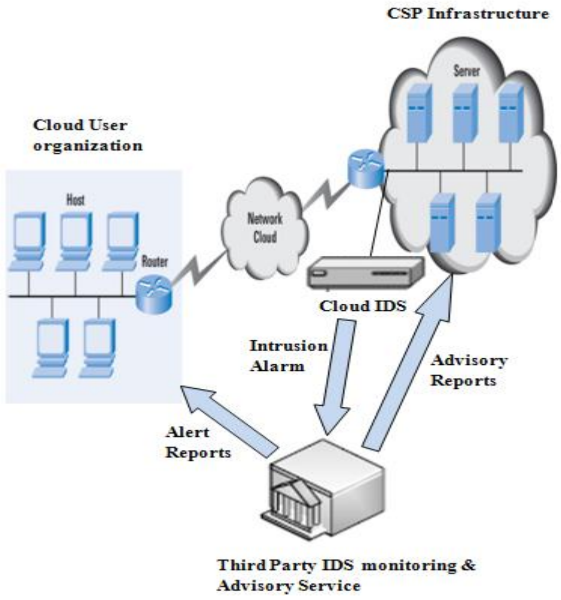

Figure 2. Proposed Cloud IDS Model

Our proposed multi-threaded NIDS model for distributed cloud environment is based on three modules: capture & queuing module, analysis/ processing module and reporting module. The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set. Each process in a shared queue can have multiple threads which work in a collaborative fashion to improve the system performance. The main process will receive TCP, IP, UDP and ICMP packets and multiple threads would concurrently process and match those packets against pre-defined set of rules. Through an efficient matching and analysis the bad packets would be identified and alerts generated. Reporting module would read the alerts from shared queue and prepares alert reports. The third party monitoring and advisory service having experience and resources would immediately generate a report for cloud user's information and sends a comprehensive expert advisory report for cloud service provider. Figure 3 depicts the flow chart of proposed multi-threaded Cloud IDS.

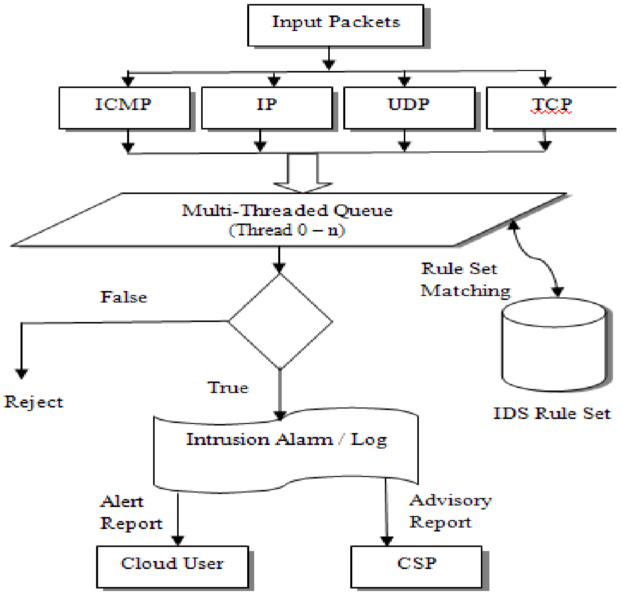

Figure 3. Flow Chart of Multi-Threaded Cloud IDS Model

6. Advantages of Proposed Model

In comparison with the traditional IDS mechanism, the proposed model has following advantages in cloud environment:

6.1. High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach.

6.2. CPU, memory consumption as well as packet loss would be reduced to improve the overall efficiency of cloud IDS.

6.3. In a host based IDS (HIDS) scenario, if host becomes the victim of offending attacker and controlled by the intruder, HIDS on that host would be compromised. In such a case the attacker would not allow HIDS to send alerts to administrator and could play havoc with the data and applications. For better visibility and resistance, network IDS (NIDS) has been proposed for cloud infrastructure.

6.4. Transparency of IDS can not be achieved by having complete control and administration of cloud IDS with the service provider. To ensure transparency of information and security of data, the cloud user must be notified of the intrusions against its virtual machine hosting data and application. A third party monitoring and advisory service has been proposed, who has both experience and resources to observe/ handle intrusion data and generate reports for cloud user as well as advisory reports for cloud service provider.

6.5. Being at a central point, proposed Cloud IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach.

7. Implementation of Proposed Model

In order to implement our proposed idea, we have carried out a simulation using .NET technology under windows environment. A system with 3.0 GHZ processor and 2 GB of RAM was used to conduct our simulation. To elaborate the function of multi-threaded IDS in cloud, we carried out a number of intrusion attacks like DOS attack on target machine. DOS attacks cause denial of services to the user through flooding traffic into the network, causing congestion to network bandwidth and declining its performance. The intruder sends multiple pings with a very short duration of time to consume network bandwidth. Threads are normally used for better system performance. A main process can segregate work to its child threads for a quick and fast processing. For testing purpose, bad packets along with legitimate data packets were sent to the simulated system. Test data is shown in Table 1. The test was conducted initially in single threaded mode, in which data packets were sent to the system multiple times and noted down the execution time (in ms). Then test data for multi-threaded mode of IDS was sent for number of times and system response time was noted. By repetitive testing and judgment, multi-threaded approach was found quick and efficient in analyzing and reporting. During the test phase it was observed that the analysis module in multi-threaded mode efficiently identified and discarded bad data packets. The reporting module generated the log reports and sent those reports to third party monitoring / advisory service for reporting and advice to the cloud users and administrators, respectively.

Table 1. Input Data Size and Execution Time

Data Size (KB)	24	50	100	200	400
Single Thread (ms)	40	82	158	296	582
Multi-Thread (ms)	28	49	112	148	286

The performance measure of multi-threaded against single threaded processing and execution time can be clearly seen by the bar graph shown in Figure 4. There is a sudden decrease in processing time during the multi-threaded mode inspection as compared to the single threaded mode inspection. Multi-threading reduces the execution time that improves upon system performance and efficiency through a cooperative and quick processing approach.

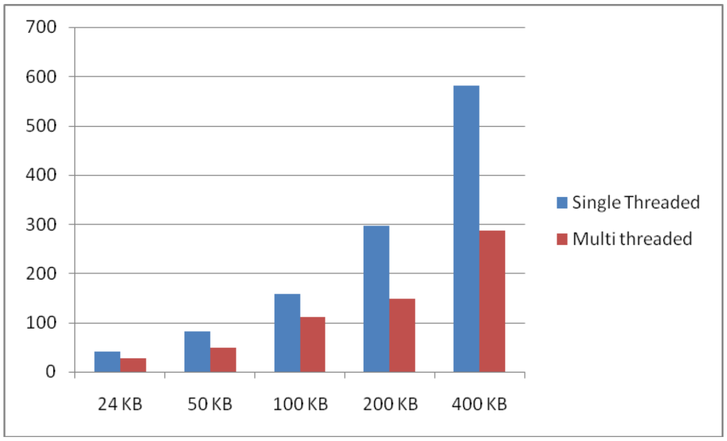

Figure 4. Performance Measure of Single Against Multi-threaded Processing

8. Conclusion

Cloud computing has innovated a new services provisioning paradigm with low infrastructure maintenance cost, scalability for data and applications, availability of data services and pay as you go features. Since cloud computing is a "network of networks" over the internet, therefore chances of intrusion is more with the erudition of intruder's attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this paper, we have proposed a multi-threaded cloud IDS which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user. We have implemented our proposed model with the help of simulation and found it to be efficient and transparent within a cloud infrastructure. For distributed nature of cloud infrastructure the ability of traditional IDSs to handle and block large malicious attacks access from offender may not be sufficient. Also the volume of data in cloud makes administrators of IDS unable to monitor every user's action.

9. Future Work

In future work, we intend to research on cloud IDS approach administered by a third party IDS provider. A third party IDS provider would be the operator of cloud IDS, by keeping configuration setting rights at its own site and cloud service provider could only view the logs information and would not be able to hide intrusion information from the user. Following this approach, the cloud user would be informed directly for intrusions that took place against its VM and data.

References

[1] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[2] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.

[3] http://en.wikipedia.org/wiki/Intrusion_detection_system.

[4] Joseph S. Sherif, Tommy G. Dearmond, “Intrusion Detection: Systems and Models”, Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02).

[5] Andreas Haeberlen,“ An Efficient Intrusion Detection Model Based on Fast Inductive Learning”, Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

[6] Richard Chow, Philippe Golle, Markus Jakobsson, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”, ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.

[7] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.

[8] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, “Integrating a Network IDS into an Open Source Cloud Computing Environment”, IEEE sixth international conference on Information Assurance and Security, 2010.

Author’s Profile

Mr. Irfan Gul is a student of MS (Computer Science) in Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST) Islamabad, Pakistan. He is a graduate in software Engineering from National University of Science and Technology (NUST) Pakistan. He is the author of “Cloud Security Auditing” research paper, published in 2nd International Conference of Next Generation Information Technology (ICNIT) 2011 (IEEE Korea). Presently, the author is working in a Government IT organization as IT manager.