International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Novel Approach to Provide Security for Cloud Data

K. Anbazhagan[1], R. Sugumar[2]

[1]Research Scholar, Department of IT, St. Peter's University, Chennai, Tamil Nadu, India

[2]Associate Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Abstract: ***Conceding security in a distributed system needs more than user authentication with passwords or digital certificates and confidentiality in data transmission. Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDOS) and Cross Site Scripting (XSS). To knob large scale network access traffic and administrative control of data and application in cloud, a novel multi-threaded distributed cloud IDS model has been proposed. The proposed cloud Intrusion Detection System handles large flow of data packets, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect intrusions.***

Keywords: Intrusions, Authentication, DDOS, XSS

1. Introduction

The term cloud is analogical to "Internet". The term cloud computing is based on cloud drawings used in the past to represent telephone networks & later to depict internet in. Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer as a service on pay-as you-use basis.

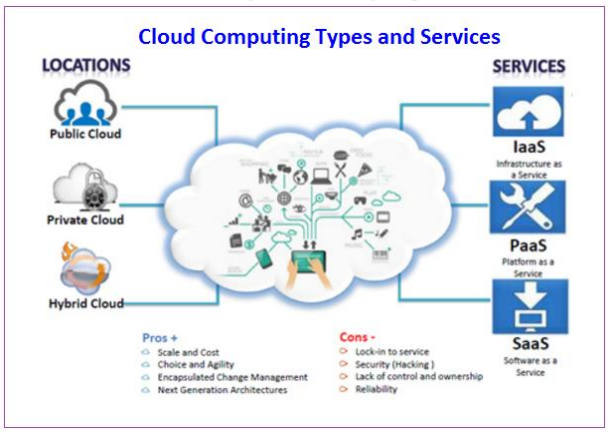

Figure 1: Cloud Types and Services

All the information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "internet cloud" without having any previous know-how on managing the resources involved. Cloud users do not own the physical infrastructure; rather they rent the usage from a third- party provider. They consume resources as a service and pay only for resources that they use. What they only need is a personal computer and internet connection. 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) [23]. 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. 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 [24]. 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.

2. Intrusions to Cloud Systems

This section illustrates several common attacks (intrusions), which causes availability, confidentiality and integrity issues to Cloud resources and services.

A. Insider attack

The person who could access the whole information system with privileged authority are defined as *insider*. Insider attacks are organized and performed by these individuals to destroy or manipulate the knowledge about system or providers and include every kind of attacks which can possibly be executed from inside [11]. Authorized Cloud users may attempt to misuse unauthorized privileges. Insiders may commit frauds and destroy information or they

may disclose information to others. This poses a serious trust issue [6].

B. Flooding attack

In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they are called as zombie (innocent host) [11]. Here, attacker tries to flood victim by sending huge number of packets from innocent host (*zombies*) in network. Packets can be either one of TCP, ICMP, UDP or a mix of these protocols. These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines are established everywhere over Internet. For this reason, exposition of cloud users with *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks are inevitable [8]. Flooding attacks affect the availability of serviced for authorized users. An attack that is realized to a server which serves one kind of service can prevent a vast of scale accessibility to this served service. These kinds of attacks are called DoS attacks. If servers' resources are slogged after flooding attacks and it prevents the execution of other services, which run on the server, this kind of attacks are called indirect DoS attacks [6].

C. User to Root attacks

In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system [11]. This makes him able to exploit vulnerabilities for gaining root level access to system For example; Buffer overflows are used to generate root shells from a process running as root. Buffer overflows are used for establish console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines [12].

D. Port Scanning

An attack that identifies open, closed and filtered ports on a system [11]. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning (same as ACK scan but it checks any modifications in the window field of packet) etc. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

E. Attacks on Virtual Machine (VM) or hypervisor

After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [11]. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. A zeroday vulnerability is a threat that tries to exploit application vulnerabilities that are unknown to others or the software developer. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates. Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [12]. A zero-day vulnerability was exploited in the Hyper VM virtualization application which resulted in destruction of many virtual server based websites [17].

F. Backdoor channel attacks

It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hackers can control victim's resources and can make it as *zombie* to attempt DDoS attack [9]. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as *Zombie* to initiate DoS/DDoS attack. For insider attacks, signature based intrusion detection solutions can normally be used [20]. To prevent attacks on VM/Hypervisor, anomaly based intrusion detection techniques can be used. For flooding attack and backdoor channel attack, either signature based intrusion detection or anomaly based intrusion detection techniques can be used [18]. Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above.

3. Intrusion Detection in Cloud Computing

As detailed in previous section, there are different types of attacks. *Intrusion Detection Systems (IDSs)* are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection, log detected information, alert or perform predefined procedures [17, 18]. They can be either hardware or software that includes whole observed computing entities. Mainly there are three types of IDS in cloud computing systems: *Host based IDS, Network based IDS, and Distributed IDS.*

A. Host-based Intrusion Detection Systems

Host-based Intrusion Detection System was the first type of intrusion detection software to be designed, with the original target system being the mainframe computer where outside interaction was infrequent [6]. Host-based IDSs operate on information collected from within an individual computer system. A Host-based IDS monitors the inbound and outbound packets from the computer system only and would alert the user or administrator if suspicious activity is detected [5] [1]. Host Based IDSs analyze the suspicious activities like system call, processes or thread, asset and configuration access by observing the situation of host. It is especially used to protect valuable and private information on server systems. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host [1]. An HIDS is not just monitor network traffic, it can also trace more and settle with local settings of an OS and log records.

B. Network-based Intrusion Detection Systems

Network-based Intrusion Detection Systems focus more greatly on the network than a specific host. Network-based

IDS detects attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts [13]. Network-based IDSs often consist of a set of single purpose sensors placed at various points in a network. Network-based IDSs (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on specified points and generally located between the end point devices like routers, firewalls [1][13]. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer [1]. OSI reference model and TCP/IP model define how these layers works and manages the traffic.

C. Distributed Intrusion Detection Systems

Distributed Intrusion Detection System (DIDS) is the way of intrusion detection in a distributed environment such as grid and cloud computing [19]. All the components in the distributed area communicate each other with an agent-based approach. There are three fundamental components and assignments are similar to other types of IDSs' components. Main subject in DIDSs deal whole system like a traditional network or host [20]. DIDS components do not have a worldwide accepted standard, but there are network and host based sensor components, detection engine and management component.

D. Network Behavior Analysis Intrusion Detection

Network Behavior Analysis Intrusion Detection (NBAD) is an intrusion detection methodology which is providing to decide if the network traffic is suspicious or not by the statistical data and formal situation of network traffic [5]. Sensors detect DoS attacks with the help of to be aware of the network traffic and unexpected application services and rule violations by scanning the network [8]. Traditional NIDSs and NBAD systems share some common components like sensors and management consoles, but NBAD systems generally do not have database servers, unlike the traditional NIDSs. NBAD systems work to decide in the case of unexpected data traffic. It is generally efficient to detect DoS attacks and worms [1].

4. System Design

Cloud computing provides application and storage services on remote servers. The clients do not have to worry about its protection and software or hardware up-gradations. Cloud model works on the model of virtualization of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine. Installing Host Based Intrusion Detection System (HIDS) in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the speedy 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 research work. 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.

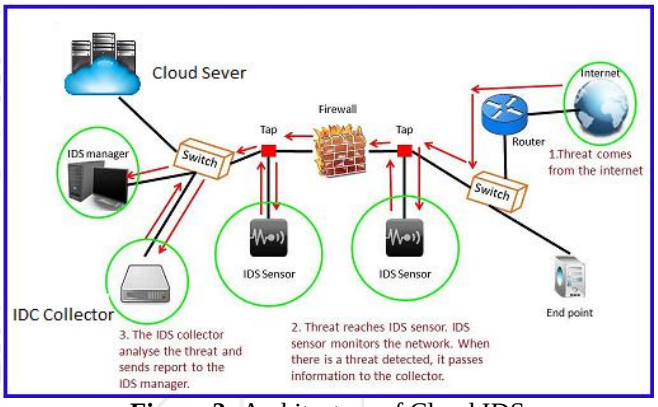

Figure 2: Architecture of Cloud IDS

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 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.

5. Advantages of Proposed Model

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

High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach. CPU, memory consumption as well as packet loss would be reduced to improve the overall efficiency of cloud IDS. 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. Transparency of IDS cannot 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. Being at a central point, proposed Cloud IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach.

6. Experimental Analysis

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.

The performance measure of multi-threaded against single threaded processing and execution time can be clearly seen by the bar graph shown in Figure 3. 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.

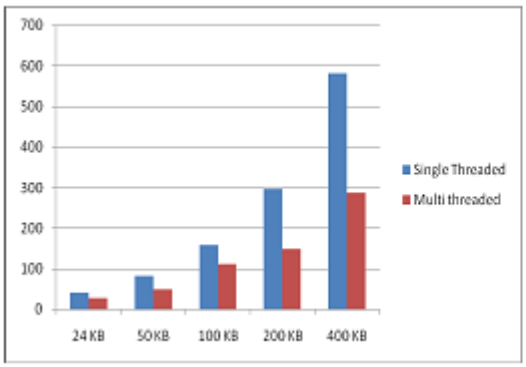

Table 1. Input Data Size and Execution Time

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

Figure 3: Performance Measure of multi Threaded against single threaded

7. Conclusion

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 report, a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user.

Reference

[1] J. Mchugh, A. Christie, and J. Allen, “Defending Yourself: The Role of Intrusion Detection Systems”, IEEE Software, 17(5), Sep.-Oct., pp. 42-51, 2000.
[2] K.V.S.N.R. Rao, A. Pal, and M.R. Patra, “A Service Oriented Architectural Design for Building Intrusion

Detection Systems", International Journal of Recent Trends in Engineering, Vol. 1(2), pp. 11-14, 2009.
[3] E-Banking - Appendix B: Glossary, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ Ebanking 04 glossary.html, Accessed on: 23/02/2012
[4] Information Technology at Johns Hopkins-Glossary G-I, http://www.it.jhmi.edu/glossary/ghi.html
[5] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE Transactions on Dependable and Secure Computing, 4(1), pp. 1-15, 2007.
[6] P. Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", IEEE 2011 World Congress on Information and Communication Technologies, pp. 456-461, 2011.
[7] Z. Mahmood, "Cloud Computing: Characteristics and Deployment Approaches", 11th IEEE International Conference on Computer and Information Technology, pp. 121-126, 2011.
[8] M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing, pp. 109-116, 2009.
[9] R. Wu, G.-joon Ahnl, and H. Hul, "Information Flow Control in Cloud Computing", IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 1-7, 2010.
[10] U. Thakar, "HoneyAnalyzer - Analysis and Extraction of Intrusion Detection Patterns and Signatures Using Honeypot", The Second International Conference on Innovations in Information Technology, Dubai, UAE September 26-28, 2005. Ashish Kumbhare et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 497-502 .
[11] H. Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", Independent Study, September 2003.
[12] W. T Work, "Intrusion Detection Systems (IDS)", National Institute of Standers and Technology, 2003, Available at: csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
[13] J. Weng and G. Qin, "Network Intrusion Prevention Systems", JTB_Journal of Technology and Business, pp. 37-49, October 2007.
[14] What is Intrusion Detection? Midmarket IT Security Definitions - Intrusion Detection, http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.html
[15] J. Nikolai, "Detecting Unauthorized Usage in a Cloud using Tenant", available at http:// www.homepages.dsu.edu/malladis/teach/717/Papers/nikolai.pdf.
[16] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", National Institute of Standards and Technology, 2001.
[17] E. Cooke, "Examination of a HIDS (SNORT + ADS)", available at:

http://csc.columbusstate.edu/bosworth/CIAE/StudentPapers/cooke.edgar.pdf..
[18] "Intrusion Detection in a Cloud Computing Environment" Available at: http:// searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment accessed on February 2012.
[19] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing",Available at: http://arxiv.org/abs/1109.5388.
[20] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International Workshop on Quality of Service, 2009 (IWQoS'09), pp. 1-9, 2009.
[21] K. Vieira, A. Schulter, C.B. Westphall, and C.M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IT Professional, 12(4), pp. 38-43, 2010.
[22] I. Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model", International Journal of Advanced Science and Technology, 34, pp. 71-82, 2011.
[23] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[24] 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.