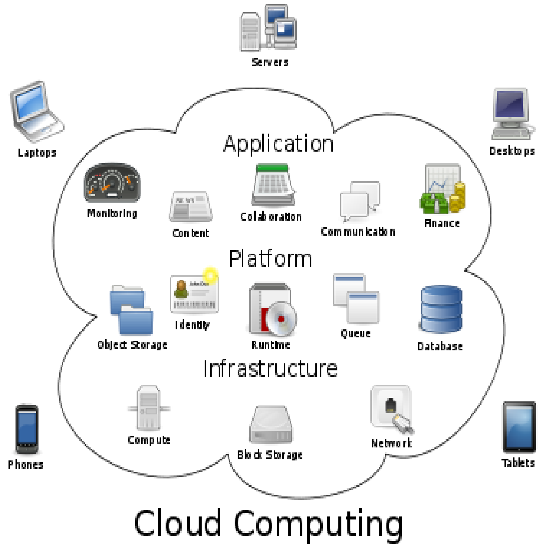
# Intrusion Detection System for Cloud Computing

Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande

Abstract:- Providing security in a distributed system requires 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 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 by integrating knowledge and behavior analysis to detect intrusions.

## 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. shows the concept [7]. All the info 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) [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. 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

1. *Ms. Parag K. Shelke, persuing the masters degree in Computer Engineering from Sipna COET, SGBAU university, Amravati (MH), India.(Author)*

   *Email parag.shelke21@yahoo.in*

2. *Ms. Sneha Sontakke, persuing the masters degree in Computer Engineering from Sipna COET, SGBAU university, Amravati (MH), India.(Co-author)*

   *Email srsontakke21@gmail.com*

3. *Dr. A. D. Gawande, Head of Department-Computer Science & Engg, Sipna COET, SGBAU university, Amravati (MH), India.(Guide)*
   *Email adgawande@rediffmail.com*

positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system. 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 [3]. 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 report, 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.

## 2. Literature Review

### 2.1 Analysis

In these days a single server handles the multiple requests from the user. Here the server has to process the all the requests from the users simultaneously, so the processing time will be high. This may leads to loss of data and packets may be delayed and corrupted. On doing this the server cannot process the query from the user in a proper manner. So the processing time gets increased. It may leads to traffic and congestion. To overcome these problems we are going for the concept called cloud computing. In this cloud computing we are going to implement the Proxy server to avoid these problems. But in this system Data Efficiency is improved but not the data security. Whenever we speak all about data efficiency we should speak about data security also, because in the cloud computing we don't know from which cloud the data is coming, so in the existing system there is no system to find the data security. The system based on the new architecture has better scalability and fault tolerance. A cluster consists of a single server and multiple proxy servers and is accessed by multiple clients. Proxy servers stores data on local disks and read or write data specified by a server. The server maintains the index for all file stored in different proxies. When a client wants to download some data, it will first send a request to the Server and the Server then redirect the request to a corresponding proxy that have the required data and hence the data will be sent to the client. With the combination of Cloud and Grid computing concepts, the data request can be efficiently serviced in a timely manner. The major part of the Project is Security, so above mentioned phase speaks all about Cloud & Grid Technology, but not about security. The Security implementation is achieved by two phase, namely -Behavioral -Knowledge

**Behavior Analysis:** Using this method, we need to recognize expected behavior (legitimate use) or a severe behavior deviation. The network must be correctly trained to efficiently detect intrusions. For a given intrusion sample set, the network learns to identify the intrusions. However, we focus on identifying user behavioral patterns and deviations from such patterns. With this strategy, we can cover a wider range of unknown attacks.

**Knowledge Analysis:** Using an expert system, we can describe a malicious behavior with a rule. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones. Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.
Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity

### 2.2 Related existing techniques

**1. Intrusion detection for grid and cloud computing**

Cloud and Grid computing are the most vulnerable targets for intruder's 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. [5] 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.

### 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 the 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.

### 2.3 Security Issues in Cloud Computing:

Security threats can be categorized as follow [4];

### 1. 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.

### 2. 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.

### 3. 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

### 4. 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.

## 3. Proposed Model:

### 3.1 Work

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 [6]. 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.

The proposed model is shown in the following figure;

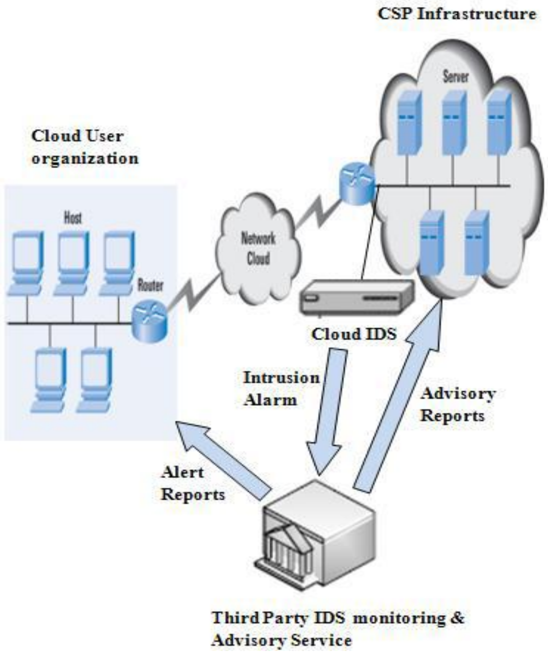


Figure 2. Proposed Cloud IDS Model [6]

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 [6].

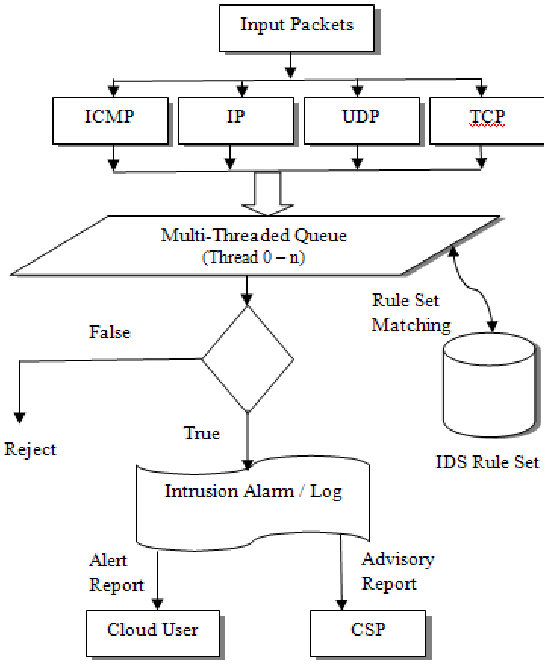


Figure 3. Flow Chart of Multi-Threaded Cloud IDS Model [6]

### 3.2 Advantages of proposed model

**1.** High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach.
**2.** CPU, memory consumption as well as packet loss would be reduced to improve the overall efficiency of cloud IDS.
**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.
4. 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.
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.

## 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.

## Acknowledgment

The making of the paper needed co-operation and guidance of a number of people. We therefore consider it our prime duty to thank all those who had helped us for making it successful. It is our immense pleasure to express our gratitude to Dr. A. D. Gawande (head of department-Computer Science and Engineering) as a guide who provided us constructive and positive feedback during the preparation of this paper. Last but not least, We are thankful to our friends and library staff members whose encouragement and suggestion helped us to complete our seminar. We are also thankful to our parents.

## 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] 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.

[4] 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.

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

[6] Irfan Gul, M. Hussain, “Distributed cloud intrusion detection model”, International Journal of Advanced Science and Technology Vol. 34, September, 2011.

[7] http://en.wikipedia.org/wiki/Cloud_computing.