DOI: https://doi.org/10.53555/nncse.v2i4.455 **Publication URL: http://nnpub.org/index.php/CSE/article/view/455**

REVIEW PAPER ON ATTACK TYPE AND INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING

Manoj Kumar Soni[1]*, Mrs. Megha Singh[2]
*[*1]M. Tech Scholar,Department of Computer Science, CIIT, Indore (M.P.), India*
[2]H.O.D. Department of Computer Science, CIIT, Indore (M.P.), India
[1]manojsonikgn@rediffmail.com ,[2]maggii.megha@gmail.com*

***Corresponding Author: -**
Email ID - manojsonikgn@rediffmail.com

Abstract: -

In any information system intrusions are the activities that damage the security and integrity of the system. Over the past few decades the network based system has grown at an explosive rate with innovations in communication and information technologies. While the computer network and their related applications brought the world together by bridging the information gap among people, it has also made it easier to leads unauthorized activity not only from external attackers but also from internal attackers, such as disgruntled employees and people abusing their privileges for personal gain. In this review paper we will try to traverse Cloud, Characteristics of Cloud, Application of Cloud, and Security issues related to Cloud. There is technique IDS which is used to detect Intrusion, we have to study this system with cloud computing concern. IDS should be used on Cloud model in a very effective way to sort out some security related challenges.

Key words: *-Cloud, IDS, Security, Attacks, Host, Firewall.*

I. INTRODUCTION:

Cloud computing is a very new technology. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. Many companies engaging in online business activities unfortunately do not see security as an important issue. From a business standpoint this may be because the return of investment in security is not immediately noticed. Additionally, implementing security tools such as IDS within an organization may be very expensive. These costs are definitely prohibitive to many small sized organizations. Thus, a study is required to be able to make an effective decision in selecting an intrusion detection system.

1. **Cloud:** In cloud computing, the word "cloud" is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet.
2. **Service Models of Cloud:** Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on requirements.**[1]** The primary service models being deployed (see Figure 1) are commonly known as:
   - **Software as a Service (SaaS)** — Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud. Also, Microsoft is expanding its involvement in this area, and as part of the cloud computing option for Microsoft® Office 2010, its Office Web Apps are available to Office volume licensing customers and Office Web App subscriptions through its cloud-based Online Services. **[1]**
   - **Platform as a Service (PaaS)** — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed. **[1]**
   - **Infrastructure as a Service (IaaS)** — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure. Also known are the various subsets of these models that may be related to a particular industry or market. Communications as a Service (CaaS) is one such subset model used to describe hosted IP telephony services. Along with the move to CaaS is a shift to more IP-centric communications and more SIP trunking deployments. With IP and SIP in place, it can be as easy to have the PBX in the cloud as it is to have it on the premise. In this context, CaaS could be seen as a subset of SaaS. **[1]**

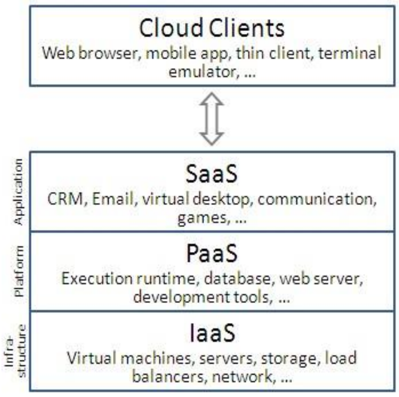

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig. 1: Services of Cloud

3. Types of Cloud:

- **Private cloud:** Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.[2] Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to re-evaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities.[3] Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".[4][5]

- **Public cloud:** A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.[6] Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Saasu is a large public cloud. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.[7]

- **Hybrid cloud:** Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.[2] Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

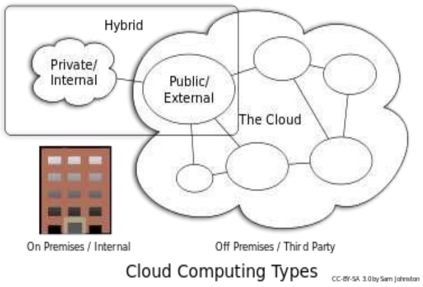


Fig. 2: Types of Cloud

4. Security in Cloud:

The key security constructs on the basis of which security policies will be defined and enforced are infrastructure, information, identity, and end-user devices. Residing on a combination of public clouds and on-premise virtualized infrastructure, workloads are decoupled from their underlying infrastructure. In the borderless enterprise, flexible and secure information controls require policies that use rich information classification models, federated identities, and context–based authorization.[8]

A cloud provider's security model should include: Physical security:

- All areas within the data centre are monitored 24x7x365 by closed-circuit cameras and on-site guards.
- Data centre space is physically isolated and accessible only by authorized administrators.
- Access is restricted to authorized personnel by two-factor biometric authentication
- CCTV digital cameras cover the entire centre, including cages, with 24x7 surveillance and audit logs. [8]

Software security:

- Cloud orchestration technology should enforce multi-tenant security across all cloud functions; it should support role-based permissions, enabling clients to define which functions can be managed by which users within their organization.
- A fully managed intrusion detection system using signature, protocol and anomaly-based inspection provides network intrusion detection monitoring.
- No passwords are stored in clear text on any system. [8]

Infrastructure security:

- Edge-to-edge security, visibility and carrier-class threat management and remediation compares real-time network traffic against baseline definitions of normal network behavior, immediately flagging all anomalies due to security hazards such as: Denial of service and distributed denial of service attacks, worms or botnets; and Network issues such as traffic and routing instability, equipment failures, or misconfigurations.
- Infrastructure systems are fully updated and patched at all times. This approach ensures both the infrastructure and operating system images remain up to date. [8]

Common Security questions that should be ask to cloud provider [8]:

- Do you provide dedicated physical or virtual LANs to your clients?
- How does your data centre architecture contribute to client security?
- Are clients able to define their own authorization and access control lists?
- How can clients ensure that their networks are secure?
- How do you provide secure access (SSL-based VPNs) to your clients?
- How do you provide account-based security?
- Do you support role-based access controls?
- Do you support the addition and removal of ACL firewall rules directly in addition to host-level security?
- How do you monitor and report on usage and activities for audit purposes?
- What compliance certifications does your company hold, and how often do you undertake a compliance audit?
- Do you permit clients to audit your security controls?

- How do you address requests for location-specific storage to abide by data sovereignty requirements?
- Can a client's data be prevented from being moved to a non-compliant location?

5. Intrusion Detection System: The first step in securing a networked system is to detect the attack. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information.

The Intrusion Detection (ID) can be considered to be the first line of defense for any security system. [9]

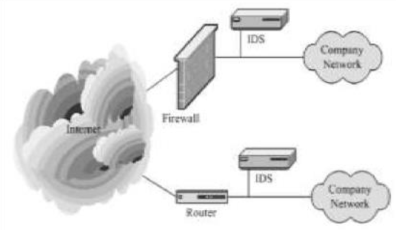


Fig. 3: IDS

As enterprise networking technology has evolved, so too have the requirements for enterprise security. What began simply as setting up a perimeter around the network using security tools like firewalls and e-mail gateways has evolved to the deployment of a wide range of tools. These include virtual private networks (VPNs) and intrusion detection systems (IDS) needed to handle the continuously growing number of threats to the network. [8]

There are two main designs available to IDSs for detecting attacks:

1) The misuse detection design

2) The anomaly detection design [10].

These two methods share many characteristics, yet are complementary in that they each have strengths where the other has weaknesses.

Knowledge-based design detects intruders by pattern-matching user activity against known attack signatures. Signatures are kept in a database containing a repertoire of information describing normal, suspicious, or attack behavior. Strength of misuse detection paradigm is that when it signals that an attack has occurred, it is very likely that an attack has actually occurred. In IDS terminology, it minimizes false positives. A weakness of misuse detection is that only attacks recorded in the database can be recognized. New attacks (and other attacks that have not yet been entered in the database) cannot be recognized. This results in failure to report some attacks (termed "false negative"). The widespread research on intrusion detection systems is due to the difficulty of ensuring that an information system will be free of security flaws [10]. The current and continuous report of newly discovered flaws and vulnerabilities in end - user and architectural systems indicates that we will likely never be able to guarantee the security of electronically transmitted information. Moreover, it strongly suggests that preventative methods will likely never be sufficient to protect our networks. Our approach combines complementary prevention (encryption) and detection (IDS) technologies to provide layered security for network traffic.

II. LITERATURE REVIEW

1. At Cloud Intrusion Detection System: Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection.

Intrusion detection and your cloud computing model

The ability to perform ID in the cloud is heavily dependent on the model of cloud computing you are using: Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection. [11]

In this technical tip, we'll discuss some of the aspects of intrusion detection (ID) that should be applied in a cloud environment. We'll talk about where ID can be applied and by whom, as well as some future ID paths that should be used when available.

Intrusion detection and your cloud computing model

The ability to perform ID in the cloud is heavily dependent on the model of cloud computing you are using:

- Software as a Service (SaaS): The reality is that SaaS users must rely almost exclusively on their providers to perform ID. You may have the option of getting some logs and deploying a custom monitoring and alerting on that information, but most ID will be done by the provider.[11]
- Platform as a Service (PaaS): Like SaaS, most of the ID for this level of service will be done by the provider. Since intrusion detection systems (IDS) are typically outside the application, you must rely on your provider to deploy IDS

in a PaaS. You can, however, configure your applications and platforms to log onto a central location where you can then set up monitoring and alerting (i.e., where you can perform ID). [11]

- Infrastructure as a Service (IaaS): This is your most flexible model for ID deployment. Unlike the other two, IaaS gives you more options as a consumer. This is where we will spend most of this article. [11]

A. Network-based Intrusion Detection System:

A "network intrusion detection system (NIDS)" monitors attack or unauthorized activity on a network. They are also called packetsniffers. They generally have a signature database against which they compare network packets. These systems have been incapable of operating in switched environments, encrypted networks and high-speed networks. An NIDS needs dedicated hardware, and forms a system which can check packets travelling on one or more network lines, in order to find out if any malicious or abnormal activity has taken place. [12]

B. Host-based Intrusion Detection System:

Host-based intrusion detection systems monitor activity on a host. They are best suited for internal threats because of their ability to monitor and react to specific user actions and file accesses on the host. They offer audit policy management centralization, supply forensics, statistical analysis, and evidentiary support. [12]

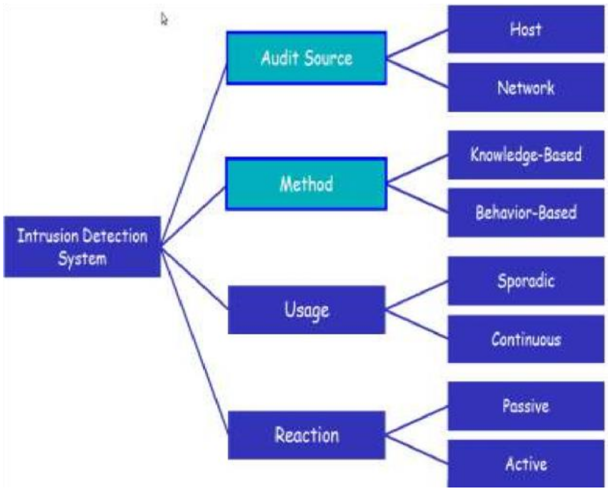
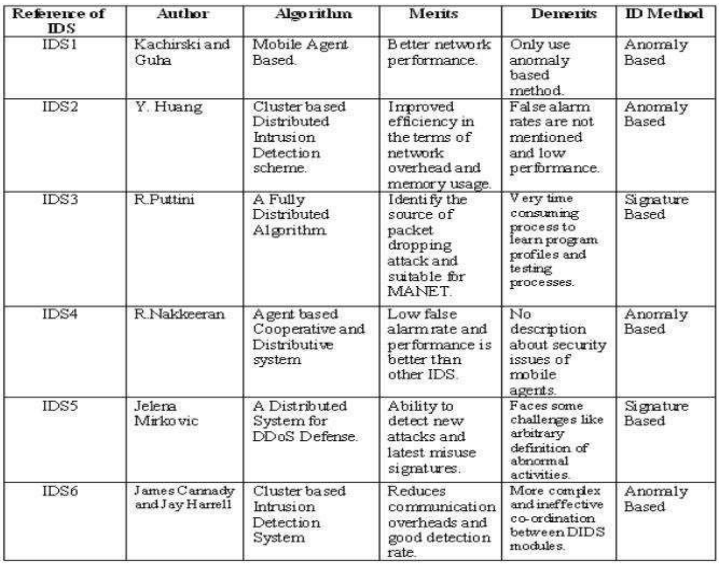


Fig. 4: IDSec

C. Hybrid Intrusion Detection System

Hybrid intrusion detection systems manage both network-based and host-based systems. They are kind of a central intrusion detection system and add a logical layer to NID and HID. [12]

2. Comparison Table:



Reference of IDS	Author	Algorithm	Merits	Demerits	ID Method
IDS1	Kachirski and Guha	Mobile Agent Based.	Better network performance.	Only use anomaly based method.	Anomaly Based
IDS2	Y. Huang	Cluster based Distributed Intrusion Detection scheme.	Improved efficiency in the terms of network overhead and memory usage.	False alarm rates are not mentioned and low performance.	Anomaly Based
IDS3	R.Puttini	A Fully Distributed Algorithm.	Identify the source of packet dropping attack and suitable for MANET.	Very time consuming process to learn program profiles and testing processes.	Signature Based
IDS4	R.Nakkeeran	Agent based Cooperative and Distributive system	Low false alarm rate and performance is better than other IDS.	No description about security issues of mobile agents.	Anomaly Based
IDS5	Jelena Mirkovic	A Distributed System for DDoS Defense.	Ability to detect new attacks and latest misuse signatures.	Faces some challenges like arbitrary definition of abnormal activities.	Signature Based
IDS6	James Cannady and Jay Harrell	Cluster based Intrusion Detection System	Reduces communication overheads and good detection rate.	More complex and ineffective co-ordination between DIDS modules.	Anomaly Based

Fig. 5: Comparison Table of different Distributed Intrusion Detection Systems (DIDS). [13]

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.

References:

[1]. Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In R. Buyya, J. Broberg, A.Goscinski. *Cloud Computing: Principles and Paradigms*. New York, USA: Wiley Press. pp. 144. ISBN 978-0-47088799-8.

[2]. "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[3]. "Is the Private Cloud Really More Securing?" CloudAndCompute.com. Retrieved 12 October 2014.

[4]. Haff, Gordon (2009-01-27). "Just don't call them private clouds". CNET News. Retrieved 2010-08-22.

[5]. "There's No Such Thing As A Private Cloud". *InformationWeek*. 2010-06-30. Retrieved 2010-08-22.

[6]. Rouse, Margaret. "What is public cloud?". Definition from Whatis.com. Retrieved 12 October 2014.

[7]. "Defining 'Cloud Services' and "Cloud Computing"". IDC. 2008-09-23. Retrieved 2010-08-22.

[8]. Data Security Monitoring in the Cloud: Challenges and Solutions, by Jeffrey Wheatman, 23 April 2012

[9]. Research on Intrusion Detection and Response: A Survey, International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005 (http://isrc.nchu.edu.tw/ijns/).

[10]. H.Debar, M.Dacier, A.Wespi, "Towards a Taxonomy of Intrusion Detection Systems",Elsevier Science B.V 31 (1999) 805-822

[11]. Firewall design and implementation and ISO 17799 and PCI compliance by Phil Cox.

[12]. Recent Trends in Security Techniques for Detecting Suspicious Activities in Computer Network: A Survey, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014

[13]. Comparative study of various Distributed Intrusion Detection Systems for WLAN, Volume 12 Issue 6 Version 1.0 May 2012 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 2249-4596 & Print ISSN: 0975-5861