Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 3, March 2020, pg.19 – 25

Understanding of Intrusion Detection System for Cloud Computing with Networking System

Sonu Devi[1]; Dr. Anuj Kumar Sharma[2]
[1]M. Tech Scholar, Department of Computer Science & Engineering
[2]Associate Professor, Department of Computer Science & Engineering
[1, 2]Om Institute of Technology & Management, Hisar

Abstract- Today, Cloud Computing is the preferred choice of every IT organization since it provides flexible and pay-per-use based services to its users. However, the security and privacy is a major hurdle in its success because of its open and distributed architecture that is vulnerable to intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect attacks on cloud. This paper provides an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect. The analysis also provides limitations of each technique to evaluate whether they fulfill the security requirements of cloud computing environment or not. We emphasize the deployment of IDS that uses multiple detection methods to cope with security challenges in cloud. A standard product provides centralized management, visibility, and control of the network. This could include the management of distributed wireless access routers or branch-office devices using centralized management in the cloud. The goal is to create and manage secure private networks by using WAN connections and a centralized management function that can reside in a data center. Connectivity, security, management, and control are pushed to the cloud and delivered as a service.

Keywords: Cloud Computing; Cloud Security; Intrusion Detection System, Network

Introduction

The architecture of cloud is open and fully distributed, making it a susceptible target for intruders. So the security of cloud environment is at risk where traditional network attacks as well as cloud-specific attacks threaten the cloud users (may be individuals or organizations).

attack, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. Traditional network security measures like firewall are better to stop many outsider attacks but attacks from within the network as well as some complicated outsider attacks (e.g. DoS and DDoS) can't be tackled effectively by using such mechanisms. This is the scenario where intrusion detection systems (IDS) come into play. The role of IDS in the security of cloud is very important since it acts as additional preventive layer of security and apart from detecting only known attacks, it can detect variants of many known attacks and unknown attacks.

The use of cloud-based networking to manage and deploy network functions across the WAN is similar to SD-WAN. The trend is broadening, as a wider array of network functions can be deployed using the cloud. The main goal is to free up services from being attached to specific hardware so that services can be deployed more quickly using software over a networking connection.

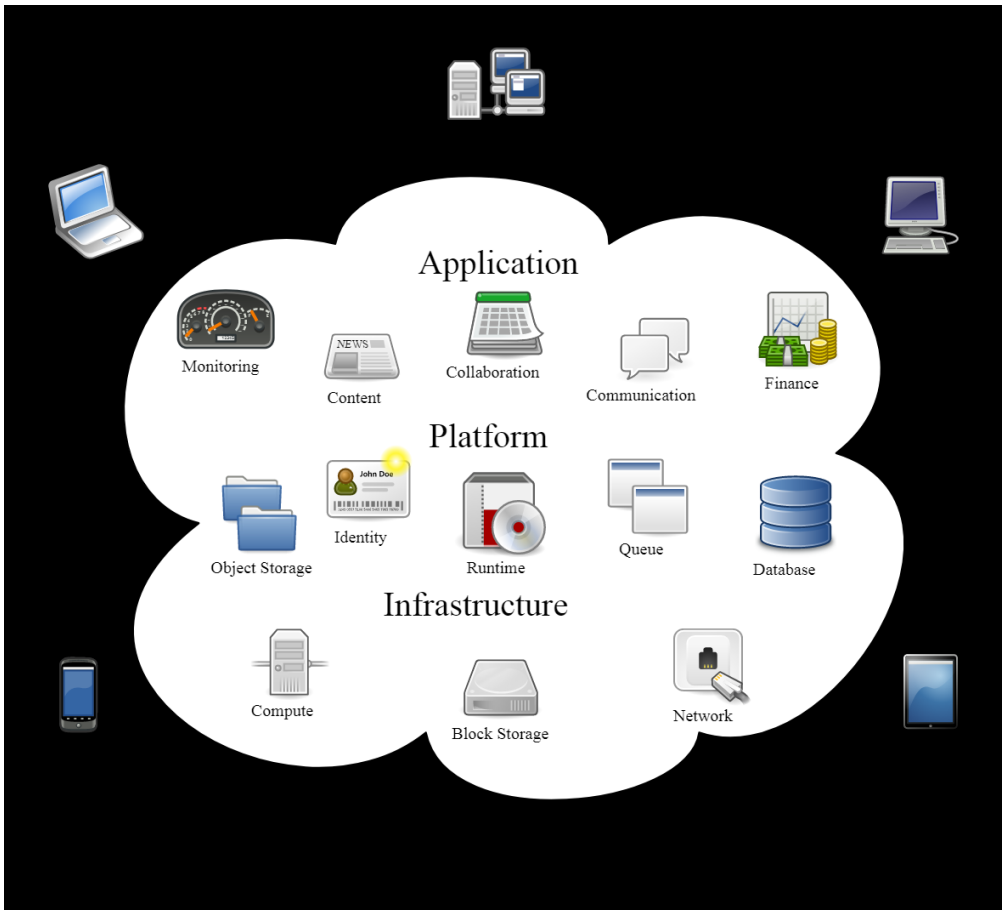
INTRUSIONS IN CLOUD

An attacker may successfully control the virtual machines by compromising the hypervisor. The most common attacks on virtual layer are SubVir, BLUEPILL, and DKSM which enable hackers to supervise host through hypervisor. Attackers target the hypervisor or VMs to access them by exploiting the zero-day vulnerabilities in virtual machines, prior to the developers' awareness about such exploits . The exploitation of a zero-day vulnerability in the HyperVM application caused damage to several websites based on virtual server.

The attacker exploits zombies for sending a large number of network packets to overwhelm the available resources. Consequently, legitimate users are unable to access the services offered over the Internet. In cloud environment, the attacker may send huge number of requests through zombies to access VMs thus disabling their availability to legitimate users which is called DoS attack . This attack targets the availability of cloud resources.

Cloud Networking

Cloud networking is a type of infrastructure where network capabilities and resources are available on demand through a third-party service provider that hosts them on a cloud platform. The network resources can include virtual routers, firewalls, and bandwidth and network management software, with other tools and functions becoming available as required. Companies can either use cloud networking resources to manage an in-house network or use the resources completely in the cloud.

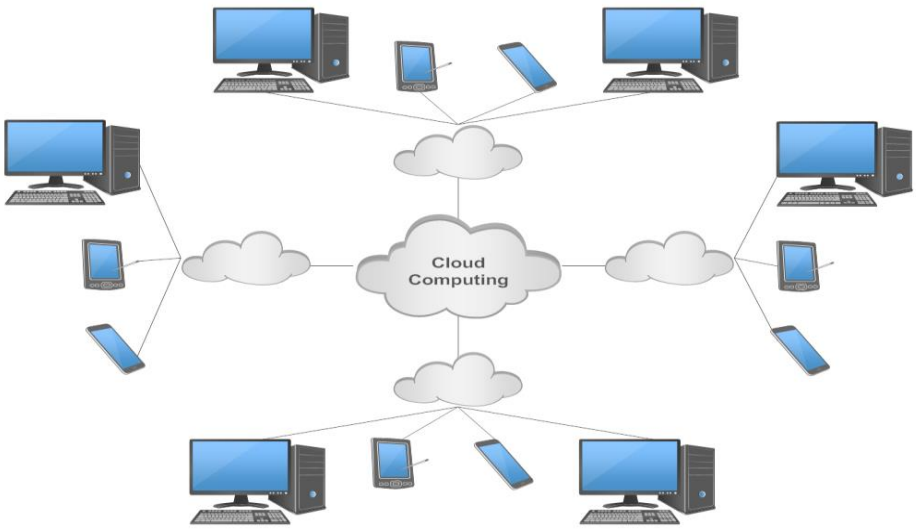


TYPES OF CLOUD-BASED IDS

Networks based IDSs (NIDS) capture the traffic of entire network and analyze it to detect possible intrusions like port scanning, DoS attacks etc. NIDS usually performs intrusion detection by processing the IP and transport layer headers of captured network packets. It utilizes the anomaly based and signature based detection methods to identify intrusions. NIDS

collects the network packets and looks for their correlation with signatures of known attacks or compares the users' current behavior with their already known profiles in real-time.

Multiple hosts in the network can be secured from attackers by utilizing a few properly deployed NIDSs. If run in stealth mode, the location of NIDS can be hidden from attacker. The NIDS is unable to perform analysis if traffic is encrypted [6]. In cloud environment, the attacks on hypervisor or VMs are detected by positioning NIDS at the cloud server which interacts with external network. However, it cannot detect attacks inside a virtual network contained by hypervisor. Cloud provider is responsible for installing NIDS in cloud [3].



Signature Based Detection

Signature based detection is performed by comparing the information collected from a network or system against a database of signatures. A signature is a predefined set of rules or patterns that correspond to a known attack. This technique is also known as misuse detection.

It can efficiently detect known attacks with negligible false alarms. Signature based method helps network managers with average security expertise to identify intrusions accurately. It is a flexible approach since new signatures can be added to database without modifying existing ones. However, it is unable to detect unknown attacks.

Signature Based IDS

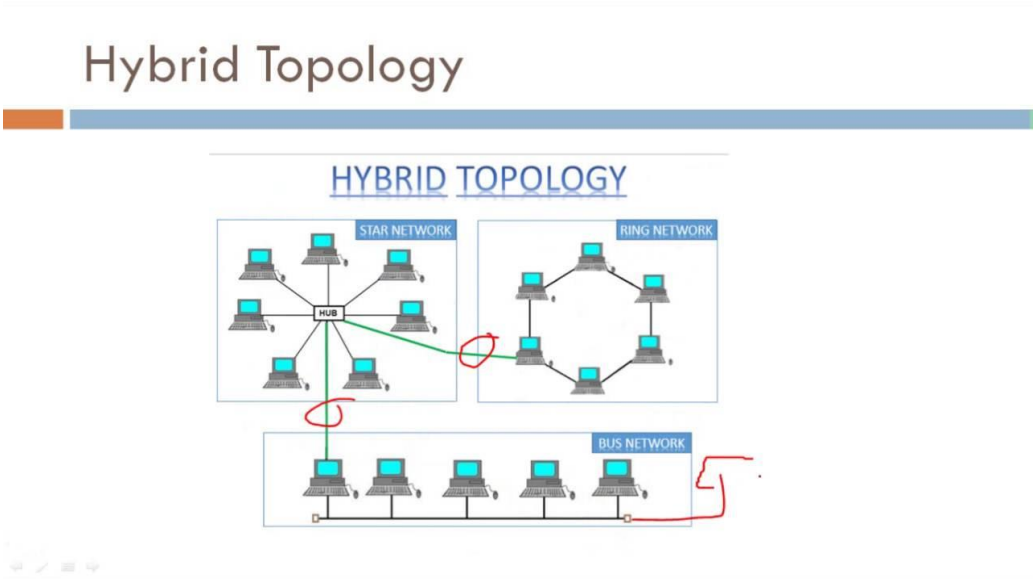
It consists of four components each with a specific role. The first one performs intrusion detection by capturing and analyzing the network packets. It instantly drops the packets exhibiting a correlation with the block table rules, or else the abnormal packets having no correspondence to these rules are forwarded to the alert clustering component which identifies the alert level of received suspicious packet. The third component blocks intrusion packets and sends alerts to other IDSs. The fourth component collects alerts from other IDSs and performs majority vote to make decision about packet. We can protect the system from single point of failure attack by deploying the proposed IDS. However, it cannot detect unknown attacks since it uses signature based detection techniques to detect intrusions.

Networking services and technologies

Hybrid connectivity

Connect your infrastructure to GCP

Cloud Interconnect, Cloud VPN, Carrier Peering, and Direct Peering provide connectivity solutions for Google Cloud Platform (GCP). Cloud Interconnect delivers an enterprise-grade connection to GCP Virtual Private Cloud. Direct Peering lets you connect directly to GCP or you can choose a partner with Carrier Peering.



Virtual Private Cloud (VPC)

Manage networking for your resources

Provision, connect, or isolate Google Cloud Platform resources using the Google global network. Define fine-grained networking policies with Google Cloud Platform, on-premises, or public cloud infrastructure. VPC network includes granular IP address range selection, routes, firewall, Cloud VPN (Virtual Private Network), and Cloud Router.

Cloud DNS

Highly available global DNS network

Cloud DNS is a scalable, reliable, programmable, and managed authoritative domain naming system (DNS) service running on the same infrastructure as Google. Cloud DNS translates domain names like www.google.com into IP addresses like 74.125.29.101. Use our simple interface, a command-line, or API to publish and manage millions of DNS zones and records.

Conclusion

The analysis shows that although different IDS techniques have already been proposed which help in detection of intrusions in cloud but they don't provide complete security. Each design lacks some features so we suggest that various detection mechanisms like signature based, anomaly based and soft computing techniques should be integrated to achieve the desired level of security in cloud. Cloud security can be greatly enhanced by utilizing soft computing techniques. However, there are still several challenges and open issues to be considered. For example, integration of IDS in VMs degrades the performance to some extent, high number of false alarms generated by anomaly based techniques, large amount of resources consumed by IDS. Lee et al. [21] has proposed a system to solve the issue of unnecessary resource consuming however, they have not provided any experimental results. In the table, we have provided the limitations of each technique. So these security challenges must be dealt before a standard framework for the security of cloud can be recommended.

In conclusion, cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses, is that it reduces

operating cost by spending less on maintenance and software upgrades and focus more on the businesses itself. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

References

[1]. C. Mazzariello, R. Bifulco and R. Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", 2010 sixth International Conference on Information Assurance and Security, pp. 265-270.

[2]. Bakshi, Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine", 2010 Second International Conference on Communication Software and Networks, pp. 260-264.

[3]. Ms. P. K. Shelke, Ms. S. Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012, pp. 67-71.

[4]. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior and C. Wills, "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System", Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), pp. 223-234.

[5]. J. H. Lee, M. W. Park, J. H. Eom, T. M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", ICACT, 2011, pp. 552-555.

[6]. V. Dastjerdi, K. A. Bakar, S. G. H. Tabatabaei, "Distributed Intrusion Detection in Clouds using Mobile Agents", Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175-180.

[7]. J. Han, M. Kamber, "Data Mining: Concepts and Techniques", 2nd edition, Morgan Kaufmann publishers, 2006.

[8]. L. M. Ibrahim, "Anomaly Network Intrusion Detection System based on Distributed Time-delay Neural Network", Journal of Engineering Science and Technology, 2010, 5(4), pp. 457-471.

[9]. Y. Dhanalakshmi, I. Ramesh Babu, "Intrusion Detection using Data Mining along Fuzzy Logic and Genetic Algorithms", International Journal of Computer Science and Security, 2008, 8(2), pp. 27-32.

[10]. W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, 2004.

[11]. K. Vieira, A. Schulter, Carlos B. Westphall, and C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IEEE Computer Society, (July/August 2010), pp. 38-43.

[12]. S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, A. Misra , "Intrusion Detection System in Cloud Computing Environment", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), pp. 235-239.

[13]. S. Bharadwaja, W. Sun, M. Niamat, F. Shen, "Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System", Eighth International Conference on Information Technology: New Generations, 2011, pp. 695-700.

[14]. An Improved Weighted Clustering for Ad-hoc Network Security New by Basant Kumar Verma and Binod Kumar, 2019.

[15]. Network Security with Cryptography by Prof. Mukund R. Joshi, Renuka Avinash Karkade, 2019.

