JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A NEW APPROACH COLLABORATIVE INTRUSION DETECTION FOR MULTI-ENVIRONMENT CLOUD

[1]Shilpa S [2]Dr Prabha R
[1]Research scholar,[2]Professor
[12]Dr Ambedkar Institute of Technology, Bangalore-560056

Abstract:

People are using cloud services more today because of its popularity and the significance of the cloud is increasing exponentially.one of the challenges of cloud is that multi cloud environment which can cause lots of complexities and security is the biggest criteria. Generally Intrusion detection [ID's] is used for securing cloud computing however conventional ID's is not effective for all types all types of attacks and vulnerabilities. So this situation definitely demands need of collaborative intrusion detection [CIDS]. Even CID's has also limitations in network information aggregation so by observing stumbling blocks in conventional CID's it force us to find new sophisticated CID's framework in hybrid cloud which definitely strengthen the security of cloud computing systems.

Keywords: CIDS, HIDS, NIDS

1. Introduction

Cloud computing is the delivery of various hardware and software services over the internet through remote servers. These servers manage, store, and process data, allowing users to expand or upgrade their infrastructure and retrieve files on demand without needing to manage or maintain the systems themselves. Cloud services are provided by many companies, such as AWS, Azure, and Google Cloud Platform. These providers deploy servers globally in various locations called data centers and typically use a pay-as-you-go model to deliver services to customers.

The capabilities and breadth of cloud computing are vast, and the IT industry categorizes them into three main types to better define use cases:

a) **Software as a Service (SaaS)** – Software is owned, delivered, and managed remotely by one or more providers. SaaS allows users to access and pay for software without installing it on their own servers.

b) **Infrastructure as a Service (IaaS)** – Compute resources, along with storage and networking capabilities, are owned and hosted by providers and are available to customers on demand.

c) **Platform as a Service (PaaS)** – This includes a broad collection of application infrastructure services, such as application platforms, integration services, business process management, and database services.

With all the benefits like scalability, flexibility, cost-effectiveness, and others, cloud computing still has certain challenges and risks for organizations implementing it. So, if you are going to implement cloud computing, here are some of the challenges and risks you might face.

1.1 Types of cloud

Private Cloud: The private cloud refers to a cloud solution dedicated to a single organization. In this setup, the organization does not share cloud computing resources with any other entity. However, private clouds have some drawbacks, including high costs, difficulties with mobile access, and scalability limitations.

Public Cloud: Public cloud environments are typically created from IT infrastructure not owned by the end user. Major public cloud providers include Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure. Drawbacks of public clouds include a lack of cost control, potential security concerns, and minimal technical control.

Hybrid Cloud: A hybrid cloud combines two or more cloud environments (private, community, or public) that remain distinct but are interconnected by standardized or proprietary technologies. This setup enables data and application portability and can support use cases like cloud bursting for load balancing between different clouds.

1.2 Top Challenges and Risks

One of the challenges of cloud is that using multi-cloud environment can cause lots of complexities and to eliminate this and few other challenges companies can practice like doing research, managing vendor relationships, and re-thinking process and tooling. The Cloud is powerful and, if implemented properly, can substantially help an organization grow faster and perform better and Significance of the cloud is increasing exponentially.

Fig: Top clod challenges

2. Intrusion Detection for Securing Cloud Computing

[1]Intrusion detection is the practice of monitoring your network, servers, workstations, and other IT assets for any suspicious activity, malicious actions, or violations of some policy. A device or software application, an Intrusion Detection System monitors a network for malicious activity or policy violations. Ultimately purpose of IDSs is use to provide a security layer of defense against malicious uses of computing systems by sensing attacks and alerting users. Because it's impossible to prevent all cyberattacks, IDSs have become essential to securing cloud computing environments.

Basic IDS components include the following categories:

- Sensors Detect and send data to the system.
- Central monitoring system Processes and analyzes data sent from sensors.
- Report analysis Offers information about how to counteract a specific event.

Examples of Intrusion Detection: Traffic Regulation Policy, Restricted IP Options Policy, Perpetual Echo Policy, E-mail Notification.

There are different types of IDSs based on where the security team sets them up:

- Network intrusion detection system
- Host-based intrusion detection system
- Perimeter intrusion detection system
- VM-based intrusion detection system

However, in the cloud, it's not as easy to get a copy of the raw network traffic due to the limitations of the environment. Therefore, in the cloud, you must switch to different layers to do intrusion detection. We can consider best intrusion detection for cloud computing at three different layers:

- Cloud layer: Explore API logs.
- Network layer: Use VPC flow logs to get network traffic metadata.
- Compute (Virtual Machines, Containers, etc.): Employ host-based intrusion detection.

2.1 Conventional IDSs:

Conventional IDS [8] basically suitable for standalone systems, which is categorized as anomaly based IDS and misuse based IDS depends on the detection method we applied. Anomaly-based IDSs are best suit for detecting zero day intrusion but are prone to high false positives. Normally not best suit for detecting zero day intrusion but accuracy detection is good. Our current cloud computing networks has several multiple entry points of intension to enhance network accessibility which tends to security vulnerabilities that sophisticated attackers can exploit using advanced techniques, such as cooperative intrusions. Attackers can initiate automated attacks targeting all vulnerable services within a network simultaneously rather than focusing on a specific service. This demands need of collaborative intrusion detection.

2.2 Survey of existing IDS cloud computing:

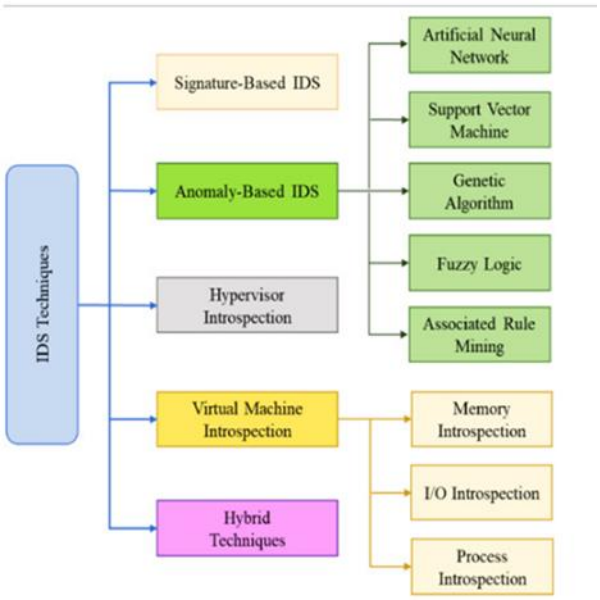

Fig: Traditional IDs in cloud computing

2.3 Need for Collaborative Intrusion Detection

Generally conventional standalone IDS are not suitable for type cooperative attacks in cloud computing environment. That's why collaborative intrusion detection systems (CIDSs) [4] are best to improve the intrusion detection efficiency. Unlike conventional standalone IDSs, a CIDS shares traffic information with the IDSs located at a local network's entry points so that IDSs can communicate directly with each other or with a central coordinator, according to the applied mode of organization. In a decentralized CIDS aggregating network information received from each IDS so that detection of malicious activity local to each IDS. Where as in hierarchical CIDS there is central coordinator who is responsible for generating a complete attack diagram of the network by aggregating information.

2.4 Limitations of Current Collaborative IDSs:

Current Collaborative IDSs has drawbacks in terms of both accuracy and efficiency moreover limited to less traffic information because single network device that only responsible for data flow in and out. In addition, the computation of network data summarization is proportional to the amount of traffic flow that single device experiences. Security is another concern for existing CIDSs. Thus, CIDSs that are designed simply by integrating conventional IDS software without proper security enhancements are vulnerable to attacks. If a CIDS is compromised, the entire cloud computing environment is in danger.

3 Collaborative Intrusion Detection Framework [3]:

By observing draw falls in existing CIDS definitely it demand new sophisticated CIDS framework could strengthen the security of cloud computing systems. And also we should perform network information aggregation in distributed and parallel by using the summarization algorithms, also need to expand their categories on demand to automatically create new clusters when they discover new types of traffic emerging. We must consider several desirable properties when designing a new CIDS framework which include fast detection of various attacks with minimal false positive rates, scalability with the expansion of the cloud computing system, self-adaption to changes in the cloud computing environment, and resistance to compromise [5].

Figure 1 shows the framework of our proposed CIDS, which meets these requirements. As Figure 1 shows, HIDSs and NIDSs cooperate to perform intrusion detection at the host and network levels, and each IDS in the network is equipped with signature- and anomaly-based detectors [6] .This tactic ensures better detection accuracy in both known and unknown attacks. There are two categories of nodes in this framework— cooperative agent and central coordinator. These nodes form a collaborative system whose security is assured through the implementation of various security mechanisms.

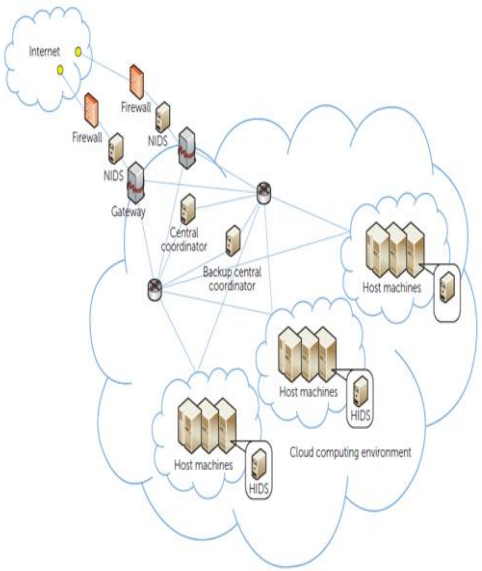

FIGURE 1: Framework of a collaborative intrusion detection system (CIDS). The figure illustrates how the different types of fellow IDSs are deployed in a cloud computing environment, and how they cooperate with each other and central coordinators in detecting intrusions. (HIDS: host-based IDS, NIDS: network-based IDS)

3.1 Cooperative Agents:

Cooperative agents are installed at either sides of HIDS or NIDS. Agents installed on a host machine to detect suspicious events are equipped with HIDSs, whereas agents installed NIDS monitoring traffic on the network. In our framework, the cooperative agents located on host machines and these host-based cooperative agents inform a central coordinator when they detect an intrusive behavior or activity. The network-based cooperative agents alert a central coordinator to any suspicious packets detected. Meanwhile, these agents summarize network traffic flowing through the network in a distributed and parallel manner and these summarizations are periodically sent to a central coordinator.

3.2 Central Coordinator:

Central coordinator aggregates the network traffic information which generates a complete attack diagram of the network of the cloud computing system. Based on this aggregation [10], the central coordinator is capable of capturing sophisticated cooperative intrusions that the individual network-based cooperative agents miss. If there is any suspicious the central coordinator raises an alert to a system administrator.

3.3 Security Mechanisms:

To ensure that the CIDS is resistant to compromise, we use authentication and encryption as well as an

integrity check. Because the CIDS works 24/7, energy-efficient group key distribution schemes are preferable for secure key distribution and node authentication. [7][8]These schemes provide a strong, secure mechanism for updating group keys when nodes join in or leave the network or a node is being compromised. The coordinators' roles can be exchanged depending on actual requirements and network conditions.

Conclusion

Current conventional collaborative ID's has drawbacks in terms of accuracy and efficiency moreover limited to less traffic information on the network but our proposed CID's framework meets the modern requirements in hybrid cloud and it suitable for all types of known and unknown attacks so that it makes more secure. It's worth noting that a hybrid detector combining misuse-based and anomaly-based detection mechanisms can help reduce the time needed to detect and enhance the detection accuracy of known and unknown attacks.

References:

[1] February 6, 2020, Best Intrusion Detection Techniques In Cloud Computing Written by: Amber Picotte.

[2] Intrusion detection system in cloud environment: Literature survey & future research directions Author links open overlay panelSuman Lata et al. 2022

[3] What Is Cloud Computing? [reference- 12 Cloud Computing Risks & Challenges Businesses Are Facing In These Days By Bernardita Calzon in Business Intelligence, Jun 1st 2022]

[4] Enhancing Big Security with Collaborative Intrusion Detection Zhiyuan Tan, University of Twente et al. SEPTEMBER 2014

[5] A. Patel et al., "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review," J. Network and Computer Applications, vol. 36, no. 1, 2013, pp. 25–41.

[6] A.K. Jones and R.S. Sielken, Computer System Intrusion Detection: A Survey, tech. report, Dept. of Computer Science, Univ. of Virginia, 2000; http://atlas.cs.virginia.edu/~jones/IDS-research/ Documents/jones-sielken-survey-v11.pdf.

[7] B. Tian et al., "A Mutual-Healing Key Distribution Scheme in Wireless Sensor Networks," J. Network and Computer Applications, vol. 34, no. 1, 2011, pp. 80–88.

[8] B. Tian et al., "Self-Healing Key Distribution Schemes for Wireless Networks: A Survey," Computer J., vol. 54, no. 4, 2011, pp. 549–569.

[9] S.N. Dhage and B. Meshram, "Intrusion Detection System in Cloud Computing Environment," Int'l J. Cloud Computing, vol. 1, no. 2, 2012, pp. 261–282.

[10] D. Hoplaros, Z. Tari, and I. Khalil, "Data Summarization for Network Traffic Monitoring," J. Network and Computer Applications, vol. 37, Jan. 2014, pp. 194–205.