ISSN:0975-9646

Architecture for Securing Virtual Instance in Cloud

Krimit Shukla [a], Harshal Trivedi [b], Parth Shah [c]

[a,c] *Computer Science and Engineering Department, Charotar University, Anand, Gujarat,India*
[b] *Computer Science and Engineering Department, Nirma University, Ahmadabad, Gujarat, India*

Abstract- **Cloud computing is computing as a utility, where services can be remotely purchased and users can store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. Here the work is to explore the possibilities to develop an effective Audit and Authentication algorithm for cloud user's data and also monitor their services. Such an auditing and monitoring service will not only helps data owners to ensure integrity but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud.**

I. INTRODUCTION

Cloud computing is not a new concept; it is originated from the earlier large-scale distributed computing technology. However, it is a sub-version technology and cloud computing is the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, it will be widely used in the near future. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud, eventually simplify the users terminal to a simple input and output devices, and bask in the powerful computing capacity of the cloud on-demand. All of this is available through a simple Internet connection using a standard browser or other connection. However, there still exist many problems in cloud computing today, a recent survey shows that data security, data integrity and privacy risks have become the primary concern for people to shift to cloud computing.

Currently IaaS providers do not provide any of the monitoring and auditing mechanisms that can be used for meeting compliance obligations. It is hard to comply with location based processing and storage requirements if the application is deployed in a public cloud because abstraction of the underlying details is a characteristic of cloud providers. The inability to monitor the cloud makes it a very difficult rather impossible choice for businesses to deploy business applications as they would not be able meet the compliance requirements resulting in huge fines or even the cancellation of their business permissions. It is therefore necessary for the IaaS Clouds to provide monitoring services and auditing logs for all instance operations. These strict logging requirements are needed to guarantee the completeness of the audit logs. It should be impossible to use Cloud resources without leaving a trace even when logged with administration privileges. IaaS should also give evidence on how to satisfy the service providers constrains. So the client can assured that his data is accessible by only him and not by other user.

Basic service models of cloud computing

Software-as-a-Service (SAAS): A business purchases software on-demand as needs arise. The software is paid for according to the number of users. Many companies prefer this approach because it can save them money on initial, upfront fees, since no applications are left unused. Getting the software required by your business is a seamless process through cloud computing because it requires only access to the Internet. There is never a need to install applications on personal computers, so companies save money by decreasing the size of their IT departments. However, the main reason companies choose SaaS is because software becomes customizable. Companies are given options for creating custom, yet professional software programs that most efficiently fit their needs. Customer relationship management (CRM) is the software solution of choice for many businesses, and is conveniently offered on the Web.

Platform-as-a-Service (PAAS) Sometimes, software applications offered through SAAS do not support the needs of a business. Perhaps, the business offers unique services, which require the use of special applications. When this is the case, PAAS may be a better alternative. PAAS provides the interface, testing environment, hosting services, and workflow facilities for building custom software and applications. This service ensures that businesses are provided with the tools they need without the risk. Highly qualified consultants facilitate the process, from initial planning to deployment. They walk users through the design process, making sure that new applications can be integrated with existing ones without complications.

Infrastructure-as-a-Service (IAAS) A more costly venture for businesses that require it is IaaS. Based on demands, a business may wish to purchase the entire infrastructure, including servers, networking, and software, and have all these resources completely outsourced. This offers more

control over networking processes to companies that desire it. Our proposed architecture allows monitoring the VM instance and execution of his data during his entire lifecycle of the virtual machine instance. It tracks the data using logging mechanism and monitors the data. By using this system the client can verify and monitor his data during entire lifecycle of VM instance in cloud any time and irrespective of location. Using this logging and monitoring mechanism at cloud provider side, it is easier for them to track the user data at in its cloud. Client can easily verify integrity of his data in the Cloud using log mechanism against unauthorized access.
Our work is focused on the above two security issues one is audit the user□s data in cloud and provide the users of cloud with logs of there virtual machines instance. Other security issue focuses on monitoring the location of services which a particular user is currently using. Both this security issues are concern for the provider and the user of cloud to ensure the integrity in cloud.

II. SECURITY ISSUES IN IAAS

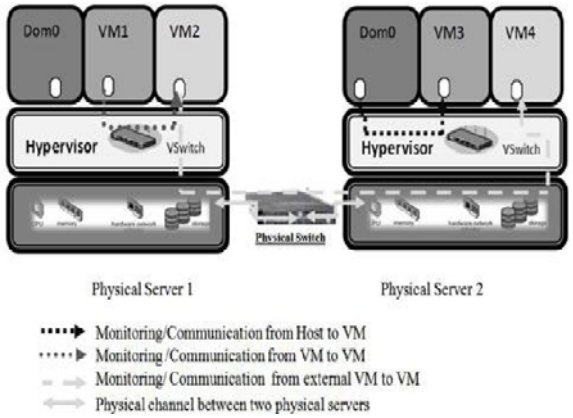

Fig 1. Interactions between VMS and host. [9]

In this Figure 1 ther is hypervisor provided to isolate the virtual machine from other user's Virtual Machine. It is possible because of hypervisor many VMs on same physical server . Hypervisor should be prevent client□s VM from other client□s VM attacks like communication, monitoring, modification, migration, mobility, auditing and Denial of Service (DoS).[9]
There are many security Vulnerabilities list below:

2.1 Communications between VMs and host

In Fig 1. shows all VMs are Communication through host. If an attacker resides on host so it is easy task for monitoring traffic of its hosted VMs. He can capture the data between VMs. If VM and host communicate with each other then attacker transfer his malicious program for modify to his data in VM. So there are issues of confidentiality and integrity of computation at IaaS. There is also issue of tampering of VM contents or inspecting VM contents. [9]

2.2 Monitoring VMs from host and Location

In host there are VMs running on it. All VMs are maintaining status like start, shutdown, pause, restart and location of there server. Any one who has privileged control over the backend can misuse this procedure. For example Xen provides hypervisor and there are many VMs running on it. It provides Xen access tool allows sysadmin to access the memory of customer,,s VM at runtime. The location of the
VMs could also be changed at runtime can violates if the location is predefined. [9]

2.3 One VM monitoring From another VM

There are many VMs running on top of the shared environment of the host. The Physical networking machines are connected by physical dedicated channel. However, in virtual networking, VMs are linked to the host machine by a virtual switch. Unfortunately, in both cases, packets sniffing and ARP poisoning could be occurred between machines. If VM modification of data is done by other VM , it could be reflect its Integrity of data. In conventional networks would solve this problem using Intrusion Detect System (IDS) but In cloud environment this tool is not appropriate for detect suspicious activity in VM due to dynamic , self service and self managed platform.[9]

2.4 Auditing of VMs

There are many VMs running on the on a single server. All the users of cloud have accesses to these VMs and store there data on this server. All the data are in the remote location and if a cloud user wants check the correctness of data or if he wants to check the log of data access to verify the integrity check there should a way user can verify these. [9]

2.5 One VM Communicate other VM

In cloud infrastructure VMs uses on shared resources. A malicious VM can potentially access other VMs through shared memory, network connections, and any other shared resources without compromising the hypervisor layer. It causes VMs from spreading viruses and other malicious. [9]

2.6 Virtual machines Mobility

The virtual machines are stored as file so it is easy to move from one physical server to other physical server. For instance, Offline attacks might be occurred by copying an offline VM over the network or to a portable storage media and access or corrupt data on their own machine without physically stealing a hard drive. In load balancing , if there are more request come one physical server then it could transfer VM to available physical server. In Live migration of VM If some attacker resides on host and copying the memory pages of the VM across the network from the source VMM to destination VMM. [9]

2.7 Denial of Service (DoS)

In This attack one VM to Consume all available resource by doing misconfiguration of hypervisor file. So that other VMs are starving for the resource. Hypervisors prevent any VM from gaining 100% usage of any shared hardware resources, including CPU, RAM, network bandwidth, and graphics memory. [9]

III. RELATED WORK

There are various tools available for monitor the cloud infrastructure. In Amazon Cloud watch provides monitoring for AWS cloud resources and the applications customers run

on AWS. Developers and system administrators can use it to collect and track metrics, gain insight, and react immediately to keep their applications and businesses running smoothly. Amazon Cloud watch can also monitor metrics that are generated by the applications you run on AWS resources. The nagios tool provides facilities like monitor applications, services, operating systems, network protocols, system metrics and infrastructure components with a single tool as shown in Fig-2.0 which was configured in our private cloud infrastructure built in eucalyptus.

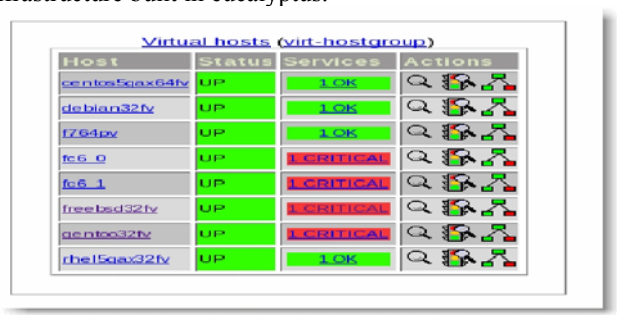

Fig 2. Nagios with virtual host [1]

There are various different tools other then this but all of them provide the same sort of functionality for monitoring such like Amazon cloud watch Api, Ganglia, Nagios.

IV. PROBLEMS IN RELATED WORK OF CLOUD COMPUTING

With these functionalities mentioned above in various tools they lacks to provide audit for files accessed on virtual machine instance and also lack in providing the current location of virtual machine from where the user is accessing the services. Below is the log file of Virtual Machine instance in eucalyptus. But it does not contain enough information through which user can retrieve useful information about file accessed or location of virtual machine. All the log files are available on servers of which a user does not have any access to view these files.

Fig 3. Output of virtual machine instance log file in eucalyptus.

Now what if a user wants to check the log of a particular file on his demand and he wants to know his location from where the Virtual machines are running. These facilities are currently not provided by cloud provider and are the major concerns of the users to switch to cloud.

V. PROPOSED ARCHITECTURE

Below is the working model of the cloud which we have proposed:

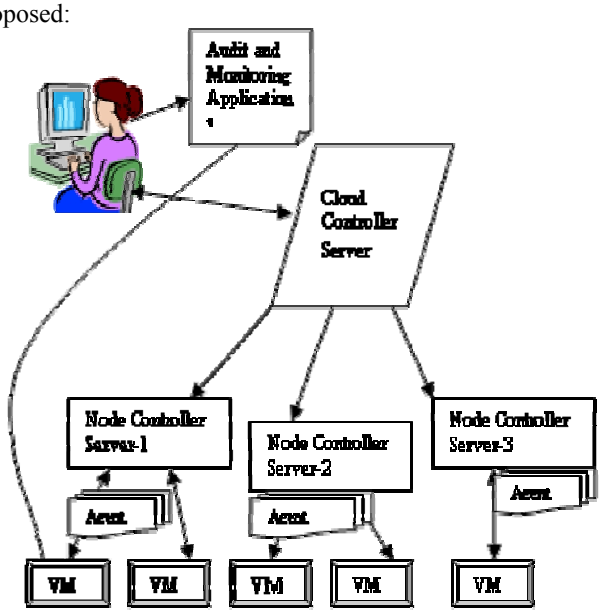

Fig 4. Proposed Architecture for monitoring virtual machine's application

Cloud Controller Server

The Cloud Controller Server (CLS) is the front end to the entire cloud infrastructure. CLS provides an EC2/S3 compliant web services interface to the client tools on one side and interacts with the rest of the components of the Eucalyptus infrastructure on the other side. CLS also provides a web interface to users for managing certain aspects of the cloud infrastructure.

Node Controller Server

A Node Controller Server (NCS) is a Virtual extension (VT) enabled server capable of running KVM as the hypervisor. The VMs running on the hypervisor are controlled by cloud server are called instances. Node Controller Server runs on each node and controls the life cycle of instances running on the node. The NCS interacts with the OS and the hypervisor running on the node on one side and the Cloud Controller on the other side.

Agent

Agents are the services which monitors and audit the Virtual machines instances at and the time when they are started. They also generate the audit log and monitoring reports that can be provided to the users on demand.

Virtual Machines (VMs)

VMs are once kind of instances of the cloud. Separate instances are created for every user on demand of services. All the services are provided to the users through instances. Instances are stored on the Node Controller Server.

User
Users are the cloud users who are access the services of the cloud.

VI. APPROACH

In the above architecture as shown in Fig 4.0 the cloud user would be accessing his services from the Cloud Controller Server once the authentication process is completed with the provided credentials. If a user puts a request for the auditing or monitoring the services the request will first go the Cloud Controller Server and request would be transferred to transfer to the node controller server where the virtual machines are running and from where different instances are provided to different users as shown in Figure 4. A monitoring agent would be continuously monitoring the activities of virtual machines. The users when requests for the details will be provided with the details of audit and location monitoring of the services on demand.

VII. CONCLUSION

As cloud computing is new area for research and development third party audit and authentication algorithm and Location Specific Virtual Machine Monitoring is a challenge for the cloud provider to ensure data integrity in the cloud for the users. Third party audit and authentication development will let the user to be rest assured about the data which is there in the cloud and it would help the cloud provider to provide data integrity support to users. The Location Specific Virtual Machine Monitoring will help the cloud users to provide location from where the cloud services are been provided to the cloud user.

REFERENCES

[1] http://linux-kvm.com/content/monitor-your-kvm-guests-nagios-virt.
[2] Amazon.com, Amazon s3 Availability Event: July 20, 2008, July 2008; http://status.aws.amazon.com/s3-20080720.html
[3] Amazon.com, Amazon Web Services (AWS), Online at http://aws.amazon.com, 2008
[4] https://help.ubuntu.com/11.04/serverguide/C/uec.html.
[5] http://www.csscorp.com/eucauecbook.
[6] http://www.open.eucalyptus.com
[7] http://www.novell.com/communities/node/2640/xen-virtual-machine-monitor-plugin-nagios
[8] Siani Pearson, Azzedine Benameur "Privacy, Security and Trust Issues Arising from Cloud Computing" 2nd IEEE International Conference on Cloud Computing Technology and science.
[9] Wesam Dawoud, Ibrahim Takouna, Christoph Meinel "Infrastructure as a Service Security: Challenges and Solutions" Ministry of Education & Higher Education, Palestine August 2008