Auditing and Monitoring of Virtual Machine Instances of Cloud

Hardik Patel [1] Yask Patel [2] Harshal Trivedi [3]
[1, 2 ,3] PG-Student
[1, 2] Information Technology Department
[3] Computer Engineering Department
[1, 2] Parul Institute of Engineering & Technology, Vadodara, Gujarat, India.
[3] Venus International College of Technology, Gandhinagar, Gujarat, India.

Abstract—The cloud computing is next generation architecture of an IT industry which provides services on demand through Internet. In contrast to the traditional approach where services are under proper physical, logical and personal controls cloud computing moves application, software and database to the large data centre where the management of the data and services may not be fully trust worthy as customer are not allowed to monitor the under-laying physical infrastructure. As cloud infrastructure span across the world, it is necessary for the data owners to track the location of server where the data actually resides as well as raise a notification when someone try to access the data. Hear we find possibilities of research work to develop an effective auditing and monitoring system for cloud users. It will help users to track the location of server in case of server crash down and process migration and also help to secure the user data by keeping data in secure premises.

Keyword: cloud computing, server location, auditing and monitoring, virtual machine, data security

I. INTRODUCTION

The term cloud computing is originated from distributed computing technology and it brings third revolution in IT industry. Cloud Computing will change fundamental trends of It industry from hardware to software, software to service and distributed service to centralize service [10].

Cloud computing is an on demand service in which shared resources, information, software packages and other resources are provided according to the clients requirement at specific time. In other words it is computing as utility where normal computers are able to perform the tasks which are beyond their limits by remotely purchasing the services through high speed internet. cloud computing reduces the processing burden of the user terminal such a way that terminal becomes a simple input and output device having good browser with high speed internet connection. This is a pay- go model where the consumers pay for the resources utilized instantly, which necessitates having highly available resources to service the requests on demand [4][10].

Cloud computing provides three basic service models.

1) Software-as-a-Service (SaaS): Any organization can purchase software or service according to their requirement and the amount to be paid for using this service is depended on the number of users. Sometimes it happens that users do not need entire software instead they just need some function of that software. At this time SaaS allows user to customize the software according to their organization's requirement. The other most importing thing about SaaS is users do not need to install any software on their local machine and can use all services through internet. SaaS service is very popular in industries as they do not need to worry about software installation and maintenance of local machines. They start saving money and time by reducing the size of IT department in an organization [4].

2) Platform-as-a-Service (PaaS): Even though SaaS provides some level of software customization Sometimes organization demands for such a unique software application that SaaS service is not able fulfill the requirement of organization. For this unique service PaaS is better option. PasS service model provides the interface, testing environment, hosting services and workflow facility so that users can develop their own software application that fulfill the needs of organization. The development of own software application requires lots of skills. For this organization hire highly qualified consultant. The consultant performs all the tasks from initial planning to the deployment. They directly provide GUI based software to the client ensuring them that this new software will integrate with the existing one [4] [10].

3) Infrastructure-as-a-service (IaaS): An expensive part of IT companies is infrastructure. To help them, cloud computing provides IaaS, Organization can purchase an entire infrastructure including servers, network, software's, storage and etc. based on requirements. This service will also help companies that have not enough space to create their own data centers [4].

Beyond this three service models, cloud computing provides four types of cloud: public cloud, private cloud, hybrid cloud and community cloud. Cloud computing has many advantages like it expands scalability, increase utilization of resources and security, lower the infrastructure costs and save energy, improve reliability and end user productivity. Users also get access to more sophisticated application.

Besides of these many advantages there are some basic issues in cloud computing like security issues, reliability issues, privacy issues, legal issues, compliance issues, data integrity issue, and long term viability issues [5][6].

In this paper the focus is on data integrity issue and in particular auditing and monitoring issue of cloud is considered. In existing system when any cloud users upload the data on cloud, Cloud system generates a notification that the particular data has been successfully uploaded on cloud. It does not provide any information about the location of the

All rights reserved by www.ijsrd.com

data. The existing system also does not generate any notification or alarm when a user data migrate from secure server location to insecure location. The user is completely unaware about what is happening to their data after once they upload data on the cloud [8] [9].

This proposed system will provide the information about the location of the server where the data actually resides as well as it will generate notification when data is migrated from secure server location to the insecure server location. The proposed system will give the latitude and longitude axis of the server where the data is actually resides. This will provide geographical location of the server so the user will come to know if the data is stored on the secure or insecure server. Once the data upload on cloud the cloud provider provides facility to select region. The regions are predefined for user to select. User can also specify the particular location of the server to store data. Our proposed system will provide information about data location on cloud. It provides status of the server, IP address of the server on which the data resides, name of region selected in which user data resides as well as country name and code. It provides specific latitude and longitude along with time zone so that user can clearly identify the specific server location. The results of the system are integrated with Google map for better user visibility.

II. RELATED WORK DONE

During the literature survey we found that some level of work is done in the auditing and monitoring area. In market some tools are available for auditing and monitor the cloud. But there is one basic problem with these all tools and is they are providing infrastructure based services. These tools provide the performance detail of the server or cloud node but they lacks to provide information about the cloud user data like location of data on cloud, and status of the server on cloud . We have examine some leading auditing and monitoring system provider which are Amazone's cloud watch, open source Ganglia and Nagios. Nagios is a powerful tool that provides user with instant awareness of user's organization's mission-critical IT infrastructure. Nagios allows user to detect and repair problems and mitigate future issues before they affect end-users and customers.

Figure. 1: Nagios XI System

Problem with existing Nagios system is it is only for IaaS [2]. Amazon Cloud watch provides monitoring for AWS cloud resources and the applications customers run on AWS. AWS enables you to monitor your AWS IaaS level resources in real-time. It also allows user to custom their application and system such as transaction volume and error rates, Access up-to-the-minute statistics, view graphs, and set alarms for user metric data.AWS does not provide any information related to cloud user data instead it provides functionality to select region only [1][7].

AWS alarms are can be set by user but it alerts only when server is down. It does not provide any mechanism for unauthorized user data access. Ganglia is a scalable distributed monitoring system for high-performance computing systems such as clusters and Grids [3]. It also provides some sort of functionality like nagios and cloud watch.

III. PROBLEMS UNREVELED

We have discussed various tools available in market for auditing and monitoring purpose but they are not efficient. The main problem is Most of the tools works fine at IaaS level for cloud administrator but lakes when it comes to audit and monitor user data in cloud. Current available tool provides detail related to Processor, Disk and Ram. So it seems not much use full for user. The agreement has been done between cloud provider and cloud user regarding to location of the server on which user data will reside. Now if user wants to check that the service provider actually follows the rules of agreement or not, or want to find out location of data uploaded on cloud, user has only way to do so is go to service provider, blindly trust them and check results what they show user. There is no direct way for user through which user can directly audit and monitor data and find out truth. The other problem is the generated log file for virtual machine instance lacks to provide useful information to user. These log files are not easily available. Even if somehow user gets access of these log file these are not in user readable form and still it remains not useful for user. These are the reason why user hesitates to migrate on cloud.

IV. PROPOSED ARCHITECTURE

The following figure shows the proposed architecture for auditing and monitoring of cloud.

– *Cloud controller server:* The Cloud Controller Server (CLS) is the front end to the entire cloud infrastructure. CLS provides web service 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) server. Node controller server runs on each node and controls the life cycle of instances running on the node. The NCS interact with the OS running on the node on one side and the cloud controller on the other side.

– *User:* Users are the cloud users who are access the services of the cloud.

All rights reserved by *www.ijsrd.com*

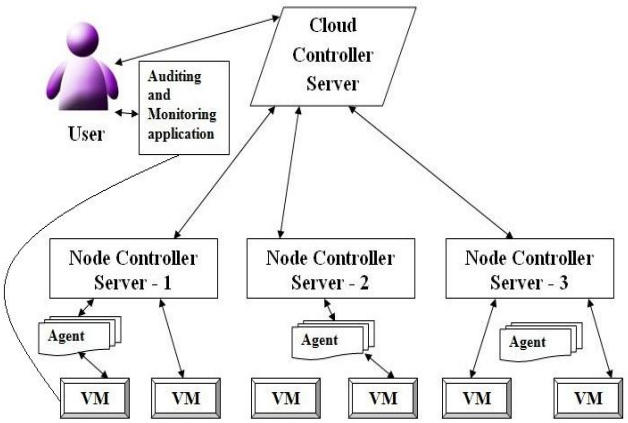

Figure. 2: Proposed Architecture for Auditing and Monitoring of Cloud.

– *Auditing and Monitoring Application:* Auditing and monitoring application will continuously monitor user data and VM and trace the location of data.

– *Agents:* Agents are the services which keeps the record of CPU usage, memory and storage space usage for each virtual instance. It also keeps the record of current number of connection to a virtual instance.

– *Virtual machines (VMs):* Virtual machines are one kind of instances of the cloud. Separate instances are created for every user on demand of services. All the services are provided to users through virtual machine instances. All instances are running on Node Controller Server.

V. APPROACH

As shown in above figure of architecture once the process of authentication for the user is get completed by comparing the credentials with the previously stored credentials, the user would be able to access his service form the cloud controller server. When a user makes a request for the auditing or monitoring service the request will first go to the cloud controller server further it will be transferred to the node controller server. Virtual machines are running on the node controller server. Node controller server is responsible for providing different virtual machine instances to different users. The task of the monitoring agent would be to monitor the activities of the virtual machines continuously. When the user ask for the details of the data it will be provided by auditing and monitoring system based on the information returned by the monitoring agent.

VI. CONCLUSION

Cloud computing is a new trend now a days in IT industry. It explores the new area for research. Security and data integrity is a main concern for cloud service provider, so development of auditing and monitoring system which provides the complete detail of data along with the location is a major challenge. Our proposed system will let the user to get assured about their data that it is on secure cloud server or not as well as it will continuously audit and monitor virtual machine and if it detects that data is migrated from secure location to insecure server location where unauthorized user can also access user data it will send alert message as a notification to cloud user. It will increase user trust in cloud.

VII. FUTURE WORK

As for the future work we have identified some issues which needed to study and resolve in depth to make this proposed auditing and monitoring system more efficient. Such as robustness, fault tolerance, security and privacy. It includes more rigorous testing of our proposed system for verity of cloud application, for cloud service providers, and for peak demand period and studies the eventual performance issues during the extreme conditions.

ACKNOWLEDGEMENT

This research work is supported in part by Parul institute of engineering and technology. Because of continuous support and encouragement from the institute this research work gets successfully completed.

REFERENCES

[1] http://aws.amazon.com/cloudwatch/
[2] http://www.nagios.com/products/nagiosxi
[3] http://ganglia.info/
[4] Qi Zhang, Lu Cheng and Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", J Internet Serv Appl (2010), Springer, Pp 7-18.
[5] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Atanu Rakshit, "Cloud Security Issues", International Conference on Services Computing, 2009 IEEE DOI 10.1109/SCC.2009.84, Pp. 517-520.
[6] Jianfeng Yang and Zhibin Chen, "Cloud computing research and security issues", 978-1-4244-5392-4/10, 2010 IEEE.
[7] Jun Feng, Yu Chen and Pu Liu, "Bridging the missing link of cloud data storage security in AWS", at the direction of IEEE Communication Society subject matter experts for publication in IEEE CCNC 2010.
[8] Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services" IEEE Network – July/ August 2010, Pp 19-24.
[9] Philippe Massonet, Syed Naqvi, Christophe Ponsard, Joseph Latanicki, Benny Rochwerger and Massimo Villari, "A Monitoring and Audit Logging Architecture for Data Location Compilance in Federated Cloud Infrastructures" 2011 IEEE International Parallel & Distributed Processing Symposium, pp 1510-1517.
[10] Krimit Shukla, Harshal Trivedi and Parth Shah, "Architecture for securing Virtual Instance in Cloud", International Journal of Computer Science and Information Technology (IJCSIT), 2012-Vol-3(3), Pp 4279-4282.
[11] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 2009 IEEE. 17th International Workshop on Quality of Service, 2009. IWQoS, IEEE, 13-15 July 2009, Charleston, SC, Pp.1-9.
[12] Shicong Meng and Ling Liu, "Enhanced Monitoring-as-a-Service for Effective Cloud Management", IEEE Transactions on Computers.

All rights reserved by *www.ijsrd.com*

[13] Meiko Jensen, Jorg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security in Cloud Computin", 2009 IEEE International Conference on Cloud Computing, Pp 109-116.
[14] Frank Doelizscher, Christoph Reich, Martin Knahl and Nathan Clarke, "Incident Detection for Cloud Environments", Emerging 2011: The Third International Conference on Emerging Network Intelligence, Pp 100-105.

All rights reserved by *www.ijsrd.com*