Indian Journal of Science and Technology, Vol 9(21) , DOI: 10.17485/ijst/2016/v9i21/95294, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Novel Technique to Control the Metering for Cloud Service using Common Deployment Model

C. Saravanakumar[1]*, C. Arun[2] and S. P. Sivasrinivasan[3]

[1]Sathyabama University, Faculty of CSE, St. Joseph's Institute of Technology, OMR, Chennai – 600119, Tamil Nadu, India; mailofcsk@gmail.com
[2]Department of ECE, RMK College of Engineering and Technology, Puduvayal, Chennai – 601206, India; carunece@gmail.com
[3]Department of CSE, Sri Venkateshwara Institute of Scienece and Technology, Chennai – 631203, India; sivzmca@gmail.com

Abstract

Background: The customers always desire to get the required services from a single cloud. It will not provide a high quality of services to the end user because all cloud services are limited to some extent i.e. lack of standard. This problem has been overcome by using the multi-cloud architecture which will provide the high quality of services with reliability. **Methods:** There are various parameters are analyzed to achieve multi cloud integration. The proposed work focuses on metering control which is a one of the parameter to manage the risk during the time of interaction. **Findings:** The common deployment model acts as a broker in various cloud interaction to achieve a high quality of services to the customer. The features are extracted from the cloud based on the services which is provided by the service provider. The services are classified and risks are assessed for selecting the suitable services from the cloud. The perfect metering gives the better confident level to the customer using the selected services. There are two essentials implemented in the customer end and provider end they are service control and service registry. The objective of the proposed system is to control the services and its interactions with the supports of cloud metering. **Application:** The risk assessment has been implemented for assessing the Quality of Service (QoS) with reliable multi-cloud interaction.

Keywords: Common Deployment Model, Cloud Control, Cloud Services, Metering, Risk Assessment

Introduction

Cloud computing is a service oriented architecture for providing the services to the customer through client server model. The core concept of cloud is a web service because all the services are accessed via open standard protocol. The services are categorized into Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These services are deployed into the cloud by using the deployment model such as private cloud, public cloud, community cloud and hybrid cloud. The cloud model follows pay-as–you-go basis model because the amount paid to the cloud provider by the customer for what they had consumed or accessed. The metering is an important factor to the customer, so the perfect metering mechanism needs to be implemented. Conventional cloud metering model only rely on single cloud which is not suitable for the customer. This problem is overcome by using the multi-cloud[2] metering technology with common standard. The common standard has been implemented using the Common Deployment Model (CDM). CDM is used to integrate various cloud service provider for sharing the services with each other. Web Coverage Processing Service (WCPS) framework is used to process the image and helps the upload of the algorithm dynamically[1]. Virtual Machine (VM) is used to allocate the resource in the data centre. A complete analysis is carried out by the VM power metering

*Author for correspondence

and also if solves the problem like VM service billing, power budgeting etc. There are different methods has been implemented in VM power metering with three-fold steps 1. Collection of Information 2. Modelling and 3. Estimation[3]. A smart grid model does not support the feature of various devices and processing during data collection. This problem has been rectified by using come method like saving of energy and cost, scalability, and elasticity. Smart-Frame model is implemented in order to construct the hierarchical data centres for data management using bid data technique. This framework supports in data confidential management based on identity but it does not support in proxy re-encryption technique[4]. The cloud customer may lose their control of the data which is already moved to the cloud service provider end. The customer data has been audited by provable data possession (PDP) technique. This technique can perform all the operations in the remote server because all customer data is stored in that location[5]. The Multi-Write Model provides on-demand file sharing feature with the support of dynamic cloud storage. A Homomorphic Authenticators technique is used for reducing and eliminating the issues and overhead during large communications[6]. A Third-Party Auditor (TPA) has been implemented for validating the integrity of the task with the support of cloud storage. The cloud storage service architecture has three elements they are user, cloud server and TPA for achieving a high availability and reliability. The main goals of dynamic operations are Storage correctness, Fast localization of data error, Dynamic data support, Dependability and Lightweight[7]. A FADE system comprises of two elements FADE clients and Key managers for managing the file access policies. This system has been deployed by using the quorum model for achieving a trust in the cloud. The customer data is protected by applying some concepts like Cryptographic protection on outsourced storage, secure storage solutions for public clouds, Access control and Assured deletion[8]. The cloud storage repair from failure is classified into two types namely transient failure and permanent failure. Transient failure is a short term failure it never resides on the cloud for a long time whereas permanent failure resides long term[9]. The PiCsMu Overlay model consists of two major elements namely PiCsMu P2P Network and PiCsMu Central Index Server by performing an indexing to the file. It comprises of entities such as File Information, Credential Information, and File Part Information[10]. The publicly verifiable Secure Cloud Storage (SCS) protocol is used to establish a relationship between the secure cloud storage and the secure network coding. SCS is a combination of five algorithms such as KeyGen, Outsource, Audit, Prove, and Verify for securing a cloud[11]. The main objective of the proposed technique is to control the services related to the metering and risk assessment. The service risks are identified based on the services which are selected by using the service controller. If there is no risks occur then the service acquires high quality otherwise it is in dangerous state which leads the performance problem.

The rest of the paper is organized are as follows: Section 2 introduces architecture of the proposed technique, and then we provide a detailed description about the algorithm and analysis of our technique in sections 3 and 4 respectively. Section 5 gives the result of the proposed technique and Section 6 conclusion and future work.

2. Proposed Method

The cloud service provider can integrate to solve the complex problem by using common deployment model. A cloud to cloud inter access will gather all the information with the properties from various cloud service providers. The features are extracted and stored into the database for assessing the cloud with sufficient performance requirement. The feature extraction phase extracts the features from the service extraction phase. The services are classified based on the features and capability. The services are estimated in various dimensions of the cloud services in order to achieve high performance. The service risk is identified by using the risk analysis phase. If any risk exists in the services, then it generates the report for handling and assessing those risks. If there is no risk, then it evaluates the reliable factor and identify the cloud service provider. The service risks are identified; the reports are generated for selecting a proper service from service providers by the user. The services without any service risk are stored into the service registry. This registry is used to control the metering and select the proper services from the cloud. The metering report is maintained in order to take the meter summery and also improve the reliability over the cloud in the customer. The service control is used to control the metering based on the assessment over service as well as risk. The customer requests are mapped into the respective cloud service provider for accessing the proper cloud services in a high reliability rate. Figure 1 shows that the system model of the proposed method.

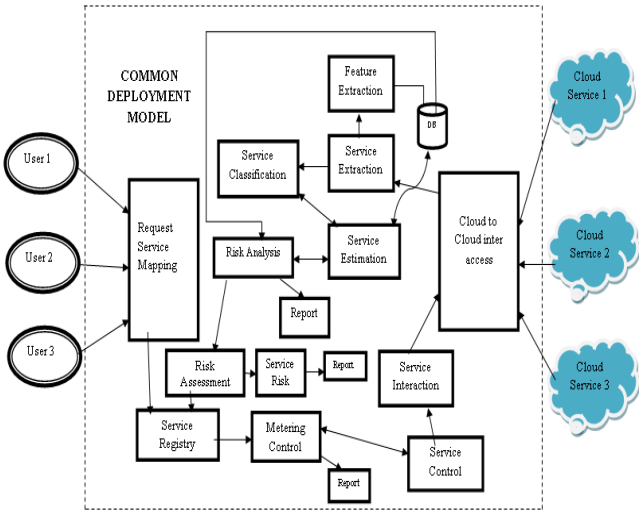

Figure 1. System Model of the proposed method.

3. Algorithm

The following algorithm gives the complete description about the proposed technique. The cloud service features are extracted and then the service risks are identified for accessing the high quality service from the cloud end. The outcome of this algorithm is a better service quality without any service risk.

Algorithm: Cloud_Metering_Control()

Input : Cloud Service Providers CSP={CSP_1…CSP_n},

Output: Metering status with Service Control;

1: SERVICES(CSP)
2: F ←{}
3: SE← {}
4: SC ← {}
5: RA← {}
6: SR ← {}
7: SI ← {}
8: Cloud Service Provider Configuration;
9: Services are extracted from cloud service provider as SE;
10: Collect the Features from the service Provider as F;
11: Extracted the relevant features from the extracted features;
12: **For each SE_i ∈ SE** do
13: **For each F_i ∈ F** do
14: Estimate the service;
15: Classify the estimated service as SC;
16: Analyze the risk for the estimated services;
17: **If risk ∈ RA** then
18: Generate the report for the risk;
19: Identify the service risk as SR;
20: **If SR_i ∈ SR** then
21: Generate the report and halt the service access;
22: **End if**
23: **Else**
24: Place the service into the service registry;
25: Request is mapped to the specific cloud service;
26: Services and metering are controlled based on the risk factor;
27: Service interaction SI is controlled by the service controller;
28: **End if**
29: **End for**
30: Return SI with Metering status;

End: Cloud_Metering_Control()

4. Analysis

The Virtual Machine (VM) properties are depends upon various factors like cores, Disk storage, Memory and Network. The cores are estimated with core speed over the number of cores. The disk storage an operation is assessed with read and writes bandwidth. The memory operation leads the latency during the cloud request and response. The transfer rate of the cloud network is based on bandwidth and latency. The following equation provides all necessary element of the proposed system

VM Properties ← { Cores U Disk Storage U Memory U Network}

Cores ← {Number_of_cores U Core_Speed}

Disk Storage ← {Number of Disks U {Disk Read Bandwidth U Disk Read Bandwidth } }

Memory ← {Memory size ← { { Read Latency U Write Latency}}

Network ← {Bandwidth, Latency}

The task is executed in the cloud can be allocated to the VM and the cost is measured according to the

VM and its execution. The CSP with properties of VM and cost is describes as follows,

Cloud Service Provider ← {Number of VM U Type of VM U Cost per Hours}

The cloud application can be categorized into name, type and component which will help to satisfy the

customer. The application component of the proposed techniques is described as follows.

Application ← {App Name, App Type, App Components}

App Components ← ***{Name, Description, Type, Value}***

The application is converted to the services in order to satisfy the customer and also fit into the cloud business standard. The service can be modeled based on the semantics of the operation parameters with necessary elements which are used to classify those services. The service parameters are discussed in the following equations,

Service place ← ***{Service Location, Name of the Service, Application}***

Service Semantics ← ***{Service Description, Binding}***

Operation Parameters ← ***{Input Parameters, Types of the parameters}***

Service Classification ← ***{Service Parameters, Operation types}***

The risk parameters can be identified with the faults from service, parameters and cloud configuration which directly relate to the performance and reliability. The risk parameter is analyzed in the following equation,

Risk Parameters ← ***{Service fault, Parameter fault, Configuration fault}***

The fault is assessed based on the cumulative count of various fault. If it is szero, then there is no risk in the service. The threshold γ is less than the fault assessment then the chance of getting risk is less where as γ is greater which leads the highest risk factor. The equations1 to 3 gives the complete details about the proposed algorithm.

$$Fault\ \ Assessment = \left\{ \begin{array}{l} \text{Fault Assessment} = \text{Count (Service fault)} + \\ \text{Count (Parameter fault)} + \text{Count(Configuration fault)} \end{array} \right\} \quad (1)$$

The service risk is assessed based on the risk which is identified during the fault assessment and risk assessment. The metering of the cloud has been controlled based on the service risk. There are two results occur during the metering control namely normal flow and stop flow.

Table 1. Physical hardware configuration

Region	Memory (MB)	Storage (MB)	Available BW	Processor Count	Processor Speed	VM Policy
0	204800	100000000	1000000	4	10000	TIME_SHARED
1	204800	100000000	1000000	4	10000	TIME_SHARED
2	204800	100000000	1000000	4	10000	TIME_SHARED
3	204800	100000000	1000000	4	10000	TIME_SHARED
4	204800	100000000	1000000	4	10000	TIME_SHARED
5	204800	100000000	1000000	4	10000	TIME_SHARED
6	204800	100000000	1000000	4	10000	TIME_SHARED

Table 2. Data center configuration

Data Center	Region	Arch	OS	VMM	VM Cost	Memory Cost	Storage Cost	Data Transfer Cost
DC1	1	x86	Linux	Xen	0.15	0.055	0.111	0.125
DC2	3	x86	Windows	Xen	0.17	0.15	0.132	0.5
DC3	4	x86	Linux	Xen	0.19	0.25	0.454	0.75
DC4	5	x86	Linux	Xen	0.2	0.35	0.65	0.155
DC5	2	x86	Windows	Xen	0.33	0.45	0.555	0.165
DC6	0	x86	Windows	Xen	0.35	0.5	0.876	0.15

$$Service\ \ Risk\ \ Assessment = \begin{Bmatrix} No\ Risk,\ Risk\ \ Assessment = o \\ Less\ Risk\ ,Risk\ \ Assessment < \beta \\ High\ \ Risk,\ Risk\ \ Assessment > \beta \end{Bmatrix} \quad (2)$$

$$Metering\ Control = \begin{Bmatrix} Normal, & (Service\ Risk\ Assessment\ U\ Risk\ \ Assessment) = 0 \\ Stop, & Otherwise \end{Bmatrix} \quad (3)$$

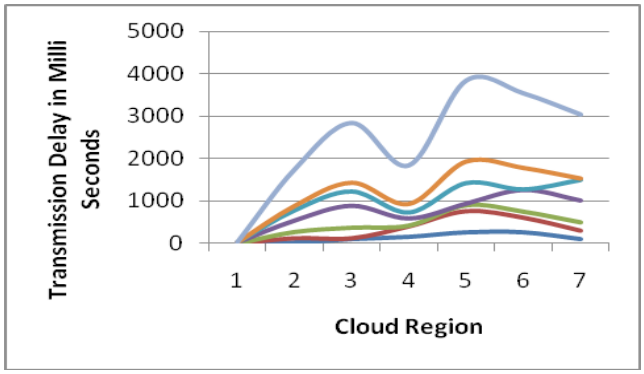

Figure 2. Transmission delay vs cloud region.

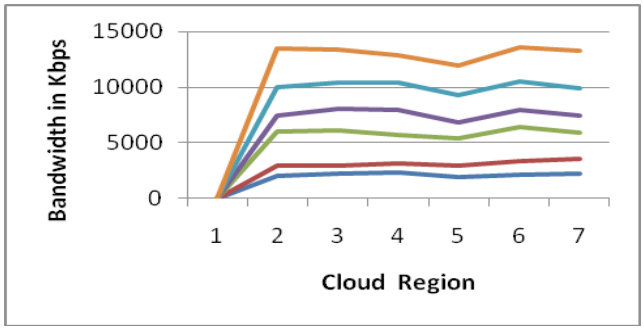

Figure 3. Bandwidth vs cloud region.

Figure 3. Risk assessment.

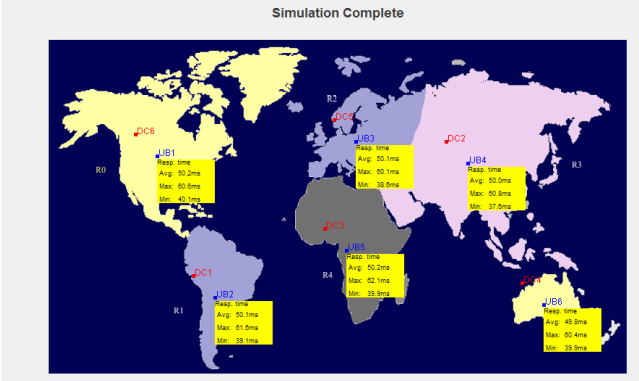

Figure 5. Simulation result.

5. Result

The result has been achieved by using the CloudAnalyst simulator which will provide the parameter for the proposed system. Figure 2 and Figure 3 shows the analysis of cloud region with transmission delay and bandwidth. Table 1 and Table 2 describes that the configuration of physical hardware and data center for cloud selection. Figure 4 shows that the analysis of risk assessment over various cloud services. Finally, Figure 5 shows that the simulation results in different location with various service providers.

6. Conclusion

The cloud is a service oriented architecture which follows the web service as a core concept and offers everything as a service. There is various service are provided by the cloud based on the deployment of the services with its region. There are plenty of cloud providers provide the services to the customer which depends on a single cloud only but the single cloud model never satisfies the customer expectation so the cloud provider should share their services to retain the customer in the cloud for a long time. This is achieved by introducing the multi cloud with various types of interaction namely multi-cloud and federation. The common deployment model has been implemented for achieving the multi cloud interaction in different perspectives. The proposed model has various processing technique they are service extraction, feature extraction, service estimation, service classification, risk analysis, risk assessment, service controlling and metering. The report is generated by this model which assesses

the violations in the services and risk threshold. The algorithm has been proposed for controlling and assessing the services and its risk. The analysis of the proposed model is done with the Cloud Analyst simulator in different parameters. The overall objective of the proposed model is to control the metering by assessing the risk in services from heterogeneous cloud.

7. References

1. Cappelaere P, Sánchez S, Bernabé S, Scuri A, Mandl D, Plaza A. Cloud Implementation of a Full Hyperspectral Unmixing Chain Within the NASA Web Coverage Processing Service for EO-1. IEEE Journal Of Selected Topics In Applied Earth Observations and Remote Sensing. 2013; 6(2):408–18.
2. Bagheri R, Jahanshahi M. Scheduling workflow applications on the heterogeneous cloud resources. Indian Journal of Science and Technology. 2015 Jun; 8(12):1–8. DOI: 10.17485/ijst/2015/v8i12/57984.
3. Gu C, Huang H, Jia X. Power metering for virtual machine in cloud computing challenges and opportunities. IEEE Access. 2014 Sep; 2(1):1106–16.
4. Baek J, Vu QH, Liu JK, Huang X, Xiang Y. A secure cloud computing based framework for big data information management of smart grid. IEEE Transactions On Cloud Computing. 2015 Jun; 3(2):233–44.
5. Barsoum AF, Hasan MA. Provable multicopy dynamic data possession in cloud computing systems. IEEE Transactions on Information Forensics And Security. 2015 Mar; 10(3):485–97.
6. Wang C, Ren K, Lou W, Li J. Toward publicly auditable secure cloud data storage services. IEEE Network. 2010 Aug; 24(4):19–24.
7. Wang C, Wang Q, Ren K, Cao N, Lou W. Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing. 2012 Jun; 5(2):220–32.
8. Tang Y, Lee PPC, Lui JCS, Perlman R. Secure overlay cloud storage with access control and assured deletion. IEEE Transactions on Dependable and Secure Computing. 2012 Dec; 9(6):903–16.
9. Chen HCH, Hu Y, Lee PPC, Tang Y. NCCloud: a network-coding-based storage system in a cloud-of-clouds. IEEE Transactions on Computers. 2014 Jan; 63(1):31–44.
10. Machado GS, Bocek T, Ammann M, Stiller B. A cloud storage overlay to aggregate heterogeneous cloud services. 2013 IEEE 38th Conference on Local Computer Networks (LCN); 2013 Oct. p. 597–605.
11. Chen F, Xiang T, Yang Y, Chow SSM. Secure cloud storage meets with secure network coding. IEEE Transactions on Computers. 2014 May:1–14.