Scalable and Secure Multi Cloud Architecture for IaaS to Address the Performance Issues

M. Sharon Evangeline
M.Tech. Scholar,
Malineni Lakshmaiah Women's Engineering College – Guntur, AP

Aluri Sai Prasad
M.Tech., Associate Professor,
Malineni Lakshmaiah Women's Engineering College – Guntur, AP

ABSTRACT
Security is an important concern to improve in emerging cloud computing to store, manage, analyze and share the sensitive data. Infrastructure as a Service (IaaS) is a provision cloud model attracting all business customers to use cloud by offering on-demand and pay-per-use hardware, storage, servers and other networking components. Present single cloud architectures are having numerous security problems like centralized data management, untrusted service providers, Honest-but-Curious cloud management etc. Multi cloud architecture was introduced recently to improve the efficiency at architecture level and to assure the sensitive data security to data owner. Recent researches were concentrated only to implement generic multi cloud architecture, which causes to raise the load balancing, elasticity and availability issues in multi cloud environment of IaaS. In this paper we introduced scalable and secure multi cloud architecture for IaaS model. This architecture addressed all issues of generic multi cloud architecture and proves that, it is most suitable one for IaaS model management.

Keywords
Multi Cloud Architecture, IaaS, Load Balancing, Cloud Security, Resource Distribution

1. INTRODUCTION
Cloud computing is offering on demand, scalable and pay-per-use SaaS, PaaS and IaaS models to cloud users. IaaS is a prominent model of cloud computing offering hardware, storage, servers and other networking components to business customers on demand through internet. This feature alleviate the burden of maintaining the own infrastructure at customer level and reduces the cost and improves the service quality. Henceforth business customers were attracted towards cloud computing IaaS model to deploy their applications and to outsource their sensitive data like health data, web account information, personal information etc. The emerging cloud computing services made data and applications of an organization from intra-organization to internationalization.

Security in cloud computing is still has to improve in certain areas like data management, trusted service provider, honest but curious management and adversaries etc. Earlier researches [2, 5, 6] were introduced many advancements in single cloud architecture to improve the security aspects. Due to the centralized data management it become complex to manage data security in single cloud architectures. Hence the complete cloud data controlled by the service provider, there is no mechanism to ensure the sensitive data security of cloud data owner. This enforces the cloud data security is subject to trust of cloud service providers and there is no guarantee that today trusts provider is always reliable.

To avoid these security problems in cloud computing recent research papers [1, 3, 4] introduced multi cloud architecture paradigm in cloud computing. This model distributes the sensitive data among multiple clouds to make individual cloud is not sufficient to access the by its own. In this case if a cloud is compromised by the adversary cannot disclose the information because of other clouds data also needed to decrypt. Due to this business customers are interested to use generic multi cloud architectures for their business needs. Multi cloud architecture is also having load balancing, elasticity and availability issues while offering the cloud services to customers.

In order to address the multi cloud environment issues, in this paper we introduced efficient and robust multi cloud architecture for IaaS model. This is an extension to the generic multi cloud architecture and especially designed for IaaS model implementation in cloud. Satisfying SLA, load balancing, elasticity, high availability, resource management and controlling are the issues of generic multi cloud environments. This architecture addressed all issues of generic multi cloud environment and proves that, it is most suitable one for IaaS model management.

2. SINGLE CLOUD VS MULTI CLOUD
Cloud environment recently upgraded to multi cloud architecture to avoid the security issues and to ensure the sensitive data protection to cloud user. This section describes the usage and advantages of single cloud architecture and multi cloud architecture.

Single Cloud Architecture: Single cloud architecture is an integrated environment, which consists of cloud platform, storage and infrastructure also as shown in fig.1. Henceforth data and process are maintained by only one cloud provider leads to more security problems. Data owners upload the sensitive data like health records to cloud storage, but they don't have the control on this data and even they don't know about whether the data is misusing or not. Present single cloud data owners don't have the proof of data security and complete cloud is under control of service provider. Hence finding the trustworthiness of a cloud service provider is an important prerequisite for cloud adoption. There are certain things may commit for data insecurity in cloud are Service Provider, honest but curious cloud employee and adversary also. Cloud service provider is the main controller of total cloud environment, so trustworthiness of provider is subjective to select the cloud provider. Recent news exploiting that some cloud service providers and employees are tampered the sensitive data from cloud storage. A part from these issues single cloud is also suffering from high cost for huge data management, data losses problems.

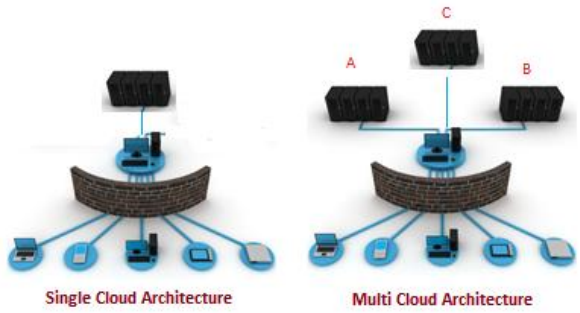


Fig.1. Single Cloud vs Multi Cloud Architecture

Multi Cloud Architecture: In order to alleviate the above security issues of single cloud architecture, Bernstien and Celesti [8, 9] proposed multi cloud architecture as a new paradigm in cloud computing. The basic idea is to use multiple distinct clouds to decentralize the data and process (logic) across multiple clouds to assure the security of data in cloud. This architecture addresses the high availability, load balancing, resource management and data security etc. In this case the cloud user data has been distributed across multiple clouds and trustworthiness of service provider is not a major aspect while integration. If any cloud compromised by an adversary is not enough to decrypt complete data, because remaining data spread across other clouds. This feature will assure the data security to data owner at cloud storage, regardless of trustworthiness of cloud owner or trust cloud. This is also helpful to integrate the individual private/public clouds together to get the integrity benefits like efficient resource management, elasticity, transparency etc. In order to secure the data among multiple clouds, this architecture uses the homomorphism in encryption and decryption while sharing the homogeneous cloud data result. Multi cloud manager is an integral part of multi cloud architecture to manage the process sharing, data sharing, result integration and load balancing etc. This node works as a master node to manage individual clouds of multi cloud architecture and schedules the jobs to dispatch among clouds to create job process pooling. The abstract multi cloud architecture designed as shown in above fig.1.

3. MULTI CLOUD ARCHITECTURE FOR IAAS

Today entrepreneurs are interested to reduce the infrastructure management cost for application maintenance by having the Infrastructure for rent. This is adoptable for temporary application management and reduces the cost for own the infrastructure at their premises. Recent cloud implementations [10 and 11] are offering services on rental basis for servers, hardware, storage area, network setup and memory as services via IaaS architecture of cloud. IaaS reduce the management burden and improves the resource utilization at cloud level to support the concept of Green Computing [7]. To avoid the security issues of single cloud architecture, recent researches [8, 9] were introducing the federation of clouds as Multi Cloud Architecture. This architecture will distribute the data and process among multiple clouds to improve the security and mitigate the process tampering. Due to this distribution of data and process among multiple clouds, multi cloud architecture is having the issues like Satisfying SLA, load balancing, elasticity, high availability, resource management and controlling etc. None of the researches were introduced the specialized architecture to implement the resource management of IaaS in multi cloud architecture.

In this paper we are introducing the scalable and robust multi cloud architecture for IaaS to address the above problems and to improve the performance of clouds to meet SLA[12]. This architecture is introducing the Multi Cloud Manager with a logical Multi Cloud Management Layer (MCML) with modules Job Scheduler, Workload Manager and Resource Manager. This layer is managed by Multi Cloud Manager which is a virtual machine only to manage the resources of multiple clouds to address the above problems.

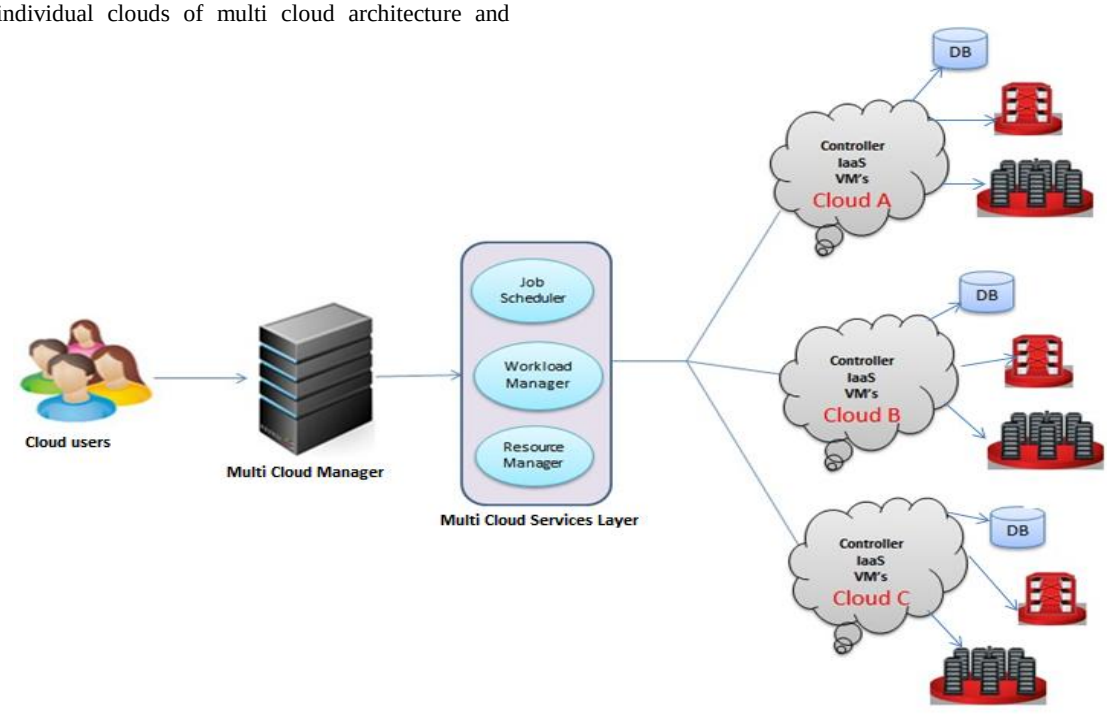


Fig.2. Multi Cloud Architecture for IaaS

Workload Manager: Previous multi cloud architecture implementation does not share the process load among multiple clouds and each cloud is only responsible to execute their own process. In our case, workload manager module implemented at MCML to allocate the jobs among the clouds based on resource availability and traffic. For example there are k different clouds c1, c2, … ck ϵ MC and each cloud is having their own, processes (jobs) are p1, p2, … pn ϵ PG which is a process group of cloud ci. Workload manager will dynamically schedule the exceeded process set Q for a cloud ci, among the rest of clouds except ci depends on their complexity and idleness. This process sharing will improve the efficiency of resource management and security of process execution in a significant manner. A process p1ϵ c1 expecting the processor time t', processor load α is less than processor capacity β (as $\alpha < \beta$) and $\{(\beta - \alpha) \geq t'\}$. If $(\beta - \alpha) < t'$ than workload manager will search the processor time availability at every cloud from c2 to cn to find the most processor time availability cloud ck. if $[ck\ (\beta - \alpha) \geq t')]$ than process p1 of c1 would be allocated to ck for processing. In this way workload manager will implement the load balancing and high availability of cloud at multi cloud architecture.

Job Scheduler: This module has to schedule the programs as per workload manager instructions in a concurrent way. Job scheduler will make the CPU time utilization efficiently to overcome bottleneck problems due to network congestion, I/O delays from user. This job scheduler uses the dynamic task scheduling algorithms [13] for job scheduling and implements the multi-tasking with parallel programming. Job scheduler initiates the lifecycle management, registers, logging and security of tasks as sown in fig.3. Once the allocation task done by workload manager, the job scheduler cares about CPU time allocation for task beginning to ending. These tasks may be data storage tasks, server tasks or process oriented tasks of any cloud of multi cloud architecture. Time slicing is the approach done by scheduler to allocate the CPU time among various tasks run by different clouds and managed by job scheduler of multi cloud architecture.

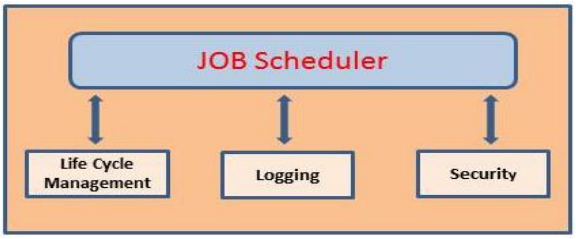


Fig.3. Job Scheduler and its responsibilities

Resource Manager: Resource manager is a logical module to manage the resource pool and resource allocation strategies. Resource pool is a collection of Databases, server resources, processing resources, Main Memory resources and Storage areas of IaaS. As per the job scheduler requirements resource manager make available the resources to allocate for process execution. Resource manager follows the dynamic resource allocation procedure to manage the resources of multiple clouds among distributed processing environments of multi cloud architecture. This efficient management helps to reduce the resource emptiness and improves the scalability of multi cloud architecture. Due to the resource sharing among multiple clouds through an integrated resource management system we can also improve the high availability of the multi cloud architecture. This implementation leads the cloud service providers to retain the response time and uptime of SLA [16]. By implementing the multi cloud architecture we can effectively address the below issues of multi cloud architecture.

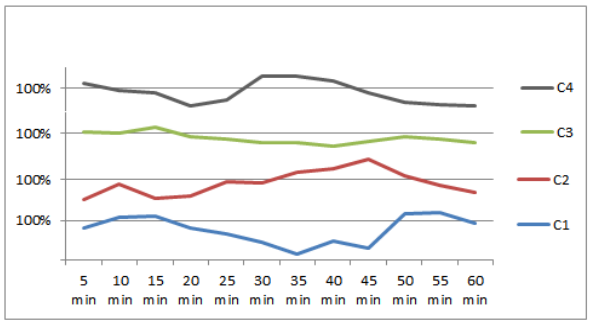
Security Issues: Security is an important concern in cloud computing to protect the sensitive data against the misusage or tampering. A data owner will upload the sensitive data (personal information) to cloud to have the cloud features like remote access, device independence, security, elasticity etc. But personalized data of cloud users is completely under control of cloud service provider who is honest but curious (HBC). Always the data security at single cloud is questionable because if a part of the cloud is compromised once the adversaries can theft the data. Due to the data is encrypted and distributed among multiple clouds, compromising of a single cloud cannot reveal the entire data or apart because of encryption and distribution. This architecture provides the robust protection to personalized cloud data and supports the secure cloud implementation.

Elasticity: Our multi cloud architecture supports the elasticity by implementing the resource sharing between multiple clouds. In this approach all clouds resources are distributable among them to face the resource underflow problem. For example, Sometimes a cloud c1 needs extra resources to run a complex operation or to handle the unexpected load from users. At that time our architecture looks at the other clouds to assess the requirement and shares the exceeded resources with c1 to avoid the resource under flow and achieves the elasticity.

High Availability: Uptime is an important parameter to measure the service Quality of a Service Level Agreement to determine the ratings of a service provider. High availability of a cloud service used to assess the uptime of a provider. This multi cloud architecture implemented the process sharing aspect among multiple clouds. In this case if a cloud is having trouble to take over a process than MCSL layer will hand over the same process to another cloud which is a part of multi cloud architecture. In this way we achieve the promised uptime efficiently and improve the high availability.

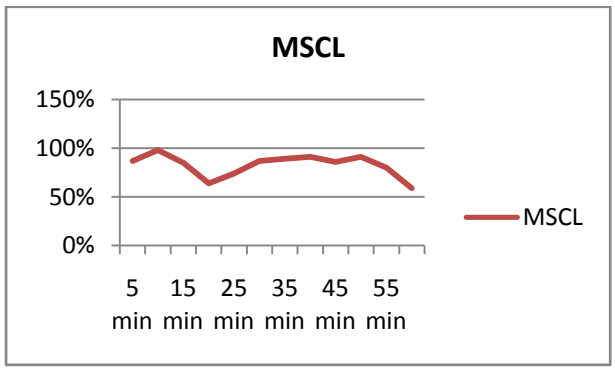
4. IMPLEMENTATION

In this section we discuss about the experiments and implementation results of Multi Cloud Architecture for IaaS. Our experiments were implemented with Cloudsim a cloud simulator tool to create the multi cloud architecture and to implement the MCSL layer for resource management to overcome load balancing, elasticity and availability issues in multi cloud environment. This tool created total 4 virtual cloud environments having core CPU's of 2.93GHz to 3.07GHz, 1TB hard disk, 8GB DDR3 RAM as hardware configuration. In order to dump the processing and resource load to clouds VC's are installed with Apache Hadoop 2.x on all of them. We implemented MCSL layer at one of the clouds as an integral part with very low amount of configuration to manage the resources of multi cloud architecture. We deployed the different types of big data mining applications to execute on virtual clouds in a real manner. These applications are having the different workloads at various time periods to create the up's and downs to test the efficiency of this project. We tested this project over 5 execution cycles with different configurations of hardware, software and workload parameters.



Graph. 1. Multi Cloud Resource Requirement Graph without MCSL layer

From the above graph we can observe that all clouds from c1 to c4 are having the hotspots and cold spots over a period of time. Hotspots are generated by resource underflow and cold spots by resource overflow of cloud architecture. From the above graph, cloud c2 is having the hotspot between 30 min – 55 min and cold spot between 5min to 25 min approximately. By the time of hotspot to continue the process execution c2 need more resources than it have, which leads to resource underflow. In this case we have to externally allocate more resources to c2 to continue the process execution. By the time of cold spot the allocated resources were not utilizing efficiently, which leads to resource overflow.



Graph. 2. Multi Cloud Resource Requirement Graph with MCSL layer

To stream line the resource overflow and underflow problems we are introducing the MCSL layer at multi cloud architecture to adjust the resources among all clouds and to retain the SLA uptime and response time promises. Graph 2 is showing the resource management results at MCSL layer of multi cloud architecture without adopting any additional resources to clouds. By utilizing the resources in an efficient manner our architecture is supporting Green Computing [7] to resist the hotspots and cold spot problems. Experiments are showing that to handle the unexpected load of process, our architecture can extend the resource capabilities, which is called as elasticity of cloud. At the end, by considering all the advantages of the MCSL layer we assure that our approach is having the high scalability, security and efficiency than traditional multi cloud architecture for IaaS.

5. CONCLUSION

In this paper we concentrated on the issues like security, elasticity, availability, resource management and resource distribution of multi cloud architecture. To address the above problems, in this paper we introduced the MCSL layer with job scheduler, workload manager and resource manager modules. This logical extension managed the resources efficiently by managing the resource pool, achieved the security by distributing the data among multiple clouds and elasticity by sharing the resources depends on workload among all cloud environments. Experiments are proving that our extension to multi cloud architecture is achieving high scalability and efficiency for IaaS of cloud.

6. REFERENCES

[1] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds,"Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD),2011.

[2] C ANETTI, R. Universally composable security: A new paradigm for cryptographic protocols. In IEEE Symposium on Foundations of Computer Science (FOCS) (2001).

[3] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD). Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 337–345.

[4] Amazon Web Services, "Amazon Elastic Compute Cloud (Amazon EC2)." [Online]. Available: http://aws.amazon.com/ec2/.

[5] M. v. Dijk and A. Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In Hot topics in Security (HotSec'10), pages 1–8. USENIX Association, 2010.

[6] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In Hot Topics in Cloud Computing (HotCloud'09). USENIX Association, 2009.

[7] http://searchdatacenter.techtarget.com/definition/green-computing

[8] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M.Morrow, "Blueprint for the Intercloud rotocols and Formats for Cloud Computing Interoperability,"Proc. Int'l Conf. Internet and Web Applications and Services,pp. 328-336, 2009.

[9] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to EnhanceCloud Architectures to Enable Cross-Federation,"Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD),pp. 337-345, 2010.

[10] Atsuo Inomata, TaikiMorikawa, Minoru Ikebe, Sk.Md. MizanurRahman: Proposal and Evaluation of Dynamin Resource Allocation Method Based on the Load Of VMs on IaaS(IEEE,2010),978-1-4244-8704-2/11.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon,R. Masuoka, and J. Molina, "Controlling data in the cloud:outsourcing computation without outsourcing control," in Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85–90, ACM, 2009.

[12] F. Raimondi, J. Skene, and W. Emmerich, "Efficient Online Monitoring of Web-Service SLAs," Proc. 16th ACM SIGSOFT Int'l Symp. Foundations of Software Eng., pp. 170-180, 2008.

[13] P. Padala, K.-Y. Hou, K. G. Shin, X. Zhu, M. Uysal, Z. Wang, S. Singhal, and A. Merchant, "Automated control of multiple virtualized resources," in Proc. of the ACM European conference on Computer systems (EuroSys'09), 2009.