

A Study on Federation Clouds and its Issues

V. Keerthi^{1*}, T. Anuradha²

¹Department of Computer Science, Dravidian University, Kupam, A.P, India

²Department of Computer Science, Dravidian University, Kupam, A.P, India

DOI: <https://doi.org/10.26438/ijcse/v8i3.109113> | Available online at: www.ijcseonline.org

Received: 09/Mar/2020, Accepted: 13/Mar/2020, Published: 30/Mar/2020

Abstract— Cloud computing which comprises various technologies from Infrastructure to Software services makes users to view computing in a new direction, as it is offering users a better IT services at low-cost. In case of collective usage of resources cloud providers that work collaboratively to form a federation of clouds or Inter-cloud. The federated cloud will address the issues like data availability, data loss, sharing of resources, data security etc. In case of resource sharing some of the applications require the credentials of the users or data to be shared between the federated clouds, which may lead to misuse of the identity, identification theft, and platform reliability. These issues are to be addressed in the federated cloud environment. An issue of security in cloud computing is an open research issue which also applied for federated clouds. In this paper we discuss some of the issues related to federation clouds and its impact on services are studied, new mechanisms and technique to be designed to reduce the risk is discussed.

Keywords—Cloud computing,Deployment models, Services,Federation,Security

I. INTRODUCTION

Cloud computing can be viewed as a new paradigm for dynamic and controlled provisioning of sharable Computing resources, maintained by state-of-the-art data centers based on network of Virtual Machines running on high powered physical machines. NIST[1] defines Cloud computing whose main design aim is to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions. Cloud can be deployed in public, private or hybrid models which provides services in various forms like Software as a Service-SaaS (e.g. Google apps, 2011), Platform as a Service-PaaS (e.g. Google app engine (2011), Microsoft’s Azure (Azure services platform, 2011)) and Infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS); Eucalyptus, 2011; Open Nebula (OpenNebula, 2011)[2] as shown in the Figure-1a,1b. Many IT Cloud service providers are moving towards federated cloud computing which allows deployment and management of cloud computing services in heterogeneous external and internal clouds to meet the business needs. The federated cloud allow customers of one cloud service can use the credentials from one service to make use of another cloud service without having the sign in separately. For decentralized storage, federated cloud is more suitable solution. In this scenario, A cluster of associated federation cloud CSP’s trade their leftover resources between each other to gain a scale of market also give high utilization of resources and expansion of their capabilities to meet customer demand at peak times[19].

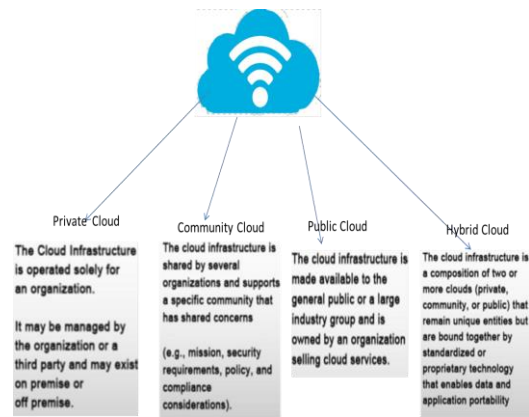


Figure-1a Cloud Computing Models

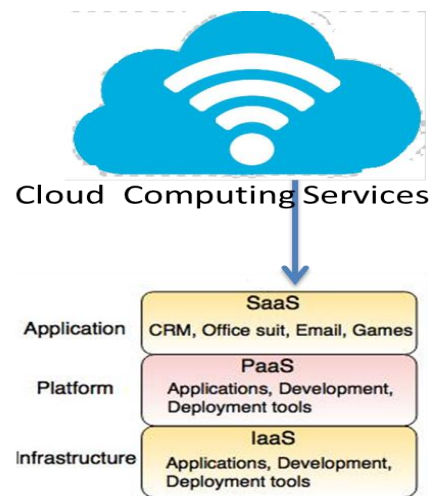


Figure-1b Cloud Computing Services

As the cloud computing is growing and its problems also, as one of the goal is high availability of data, but in single cloud there are risks of service failure or server crash which leads to data loss or attack on single cloud will make entire data under threat so in [17] also prefers the concept of “Cloud-of-Clouds” also known as “inter-clouds” or “multi-clouds” which allows data to be stored in different clouds which risk and increases data availability in which only part of data will be lost and hence improves high level of security to the confidential data. In this paper [17] various research techniques such as File sharing ,key sharing, use of byzantine protocols ,Rains clouds system ,Depsky architectures are studied and given various ways of using inter-cloud solutions and its usage.

With research is extensively carried in field of technology of Cloud Computing in recent years which has given some solutions to different security problems with different designs, models of databases, virtualization techniques and memory management but these solutions are relevant to cloud computing by taking into consideration of a few data centers at single place. But when cloud computing when combined with Big data to which the cloud technology is mostly used or applied, faces challenges in security when data is distributed across multiple cloud. The issues such as at system level, client confirmation level, exchange of data format level, SLA level and other to generic issues, strategies are studied[18], which some can be addressed by using federation of cloud .

To deliver the services efficiently cloud should possess the characteristics like Resource pooling, Virtualization, Multi-tenancy, On-demand self-service, Rapid elasticity ,metered service etc., as show in Figure-2.

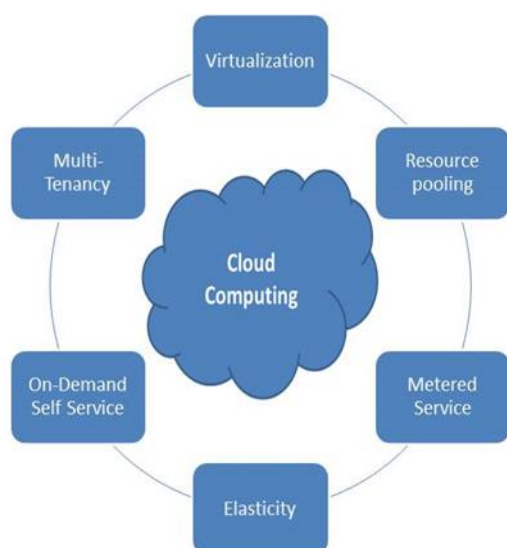


Figure-2 Cloud Computing Characteristics

The transformation of IT through cloud computing is accelerating as a wide range of organizations are adopting this new approach for deploying a variety of applications.

However, security concerns prevent many organizations from deploying certain types of applications in the cloud. They worry both about attacks on data being sent over the Internet to and from the cloud, and about whether their applications and data are more vulnerable to attack in a cloud than in their own internal computing resources.[13]

As more and more users are moving towards cloud load balancing, traffic may become a hurdle for cloud adoption so the possibility of interconnecting the cloud computing environments of two or more service providers which form as federation to solve the issue has come into practice. Inter-connection of various cloud models forms a federated cloud (also called cloud federation or may be hybrid cloud) which are deployed and managed with various multiple external and internal cloud computing services to match business needs [12]. A model of Federations of cloud may be constructed in various ways with different cloud models or topologies.

In Cloud federation aggregation of services from different providers are pooled for three basic interoperability features such as resource migration, resource redundancy and combination of complementary resources. The rest of the paper is organized as follows. In Section II related work regarding cloud and federated cloud is discussed and section III issued related cloud federation is discussed. Finally in the section IV reviews the content of this paper and presents the conclusions.

II. RELATED WORK

As in [3] Federation is the ability of multiple independent resources or cloud providers to act like a single resource for a specific purpose. Cloud computing itself is a federation of resources, with many assets, identities, configurations and other details of a cloud computing solution must be federated to make cloud computing practical. Also many issues like trust, Identity access management; Signing-in has been discussed regarding Federation of clouds. Buyya et al. in [4] suggests a cloud federation oriented has a specific purpose, just-in-time, opportunistic and scalable application services provisioning environment called InterCloud. As a result Cloud application service (SaaS) providers will have difficulty in meeting QoS expectations for all their consumers. Hence, they would like to make use of services of multiple Cloud infrastructure service providers who can provide better support for their specific consumer need in terms of speed traffic etc., this kind of requirements often arises in enterprises with global operations and applications such as Internet service, media hosting, and Web 2.0 applications. This necessitates building mechanisms for federation of Cloud infrastructure service providers for seamless provisioning of services across different Cloud providers.

In paper by Subashini and kavitha[5], has discussed various security issues at various service models like in

cloud like Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization which is also application to Federation of Cloud environment. Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. In the case of federated clouds this becomes more serious issue that is to be addressed when a computation requires an exchange of data between clouds in federation it is necessary that both privacy and integrity of data should be considered [6]. The confidentiality of sensitive data must be ensured integrity at during mixing transfer of data with other cloud hosts. If the data is shared between multiple users or clouds , the CSP must ensure data integrity and consistency. The CSP must also protect all of its cloud service consumers from malicious activities or data modification [7-8]. At high demand of resources services from different providers aggregated in a single pool supporting three

Migration, redundancy and complementation of resources which allows clients relocation to another CSP or Backup of VM's at the time of recovery or change of domains or using more aggregated resources results in flexibility [9].

The purpose of federated Cloud paradigm aimed to provide flexible and reliable services composed of a mixture of internal and external mini-clouds, but this heterogeneous composition is raising new security concerns of the customers. To overcome the fears and deal with the threats associated with outsourcing data and applications to the Cloud, new methods for security assurance are urgently required. Cloud providers should address privacy and security issues as a matter of high and urgent priority not in only in non-federation but also in federated architecture of cloud. [14].

III. FEDERATION COMPUTING

Cloud federation brings together different service providers and their offered services as single entity for the services to be rendered to clients. Cloud Federation can be viewed as horizontal and vertical federation. Horizontal federation takes place on one level of the Cloud Stack e.g., the application stack, whereas vertical federation spans multiple levels [9].

Various Cloud variants can be tailored to match different sets of customer requirements. Federation of cloud allows cloud provider to provide resources to satisfy complex application request by client as he can have more resources at his premises by collaboration. In terms of reliability, trust, and security among multiple cloud providers will be improved in federated clouds.

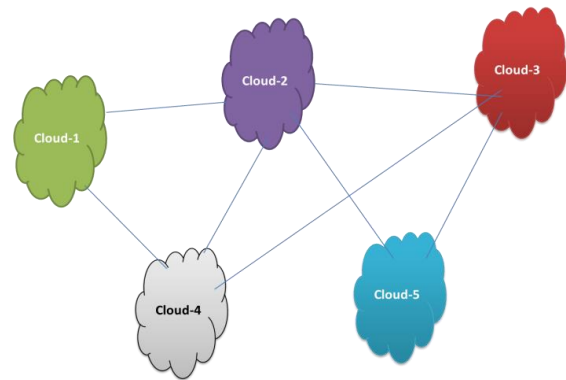


Figure-3 Federated Cloud

Scaling Federation horizontally or vertically will allow resources on the cloud to restore or to improve application performance. Vertical scaling (up) entails adding more resources to the same computing pool—for example, adding more RAM, disk, or virtual CPU to handle an increased application load. Horizontal scaling (out) requires the addition of more machines or devices to the computing platform to handle the increased demand [2].

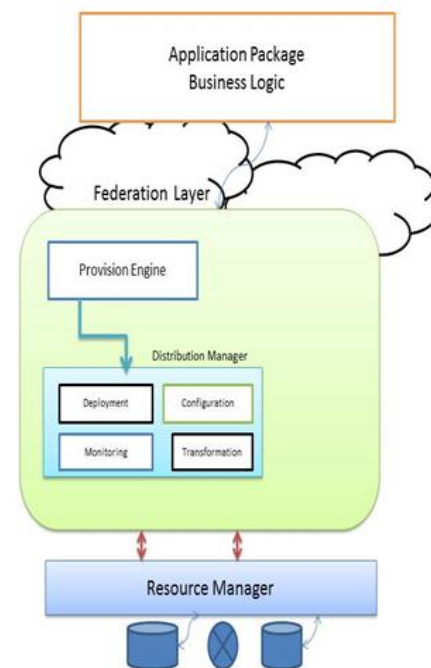


Figure 4: Federation Architecture

In federation reference architecture shown in figure-4 has following components when in federation application can be moved to one CSP to another CSP or any resource can be adjusted for client support.

a) Provisioning Engine: a Software component maps application along with policies and business logic components to a pool of resources and further executed and enforced through a Distribution Manager.

b) Distribution Manager contains multiple subcomponents that guarantees enforcement of consistency between data replica and same deployment configuration on multiple servers.

c) Resource Manager: it supports above layers by providing an abstraction of the APIs to the underlying services and allows to configure resources in different clouds in a unified way.

In Federated Cloud Management (FCM)[15] architecture for providing unified access to a federated Cloud that aggregates multiple heterogeneous IaaS Cloud providers in a transparent manner, an interoperable solution is developed where the users are able to execute services deployed on cloud infrastructures transparently, with a well-defined interface in an automated way. Virtualized resources at IaaS are stored in a generic repository called FCM Repository. FCM will automatically programmed to replicate to the native repositories of the different Infrastructures as a Service cloud providers at lower layer as in Resource Manager in fig:4 architecture discussed.

Similar to above models the Reservoir architecture [2] uses three layers, the Virtual Execution Environment Host (VEEH), Virtual Execution Environment Manager (VEEM), and Service Manager. While the names are different, there is a close functional correspondence to the layers defined in above models.

IV. CLOUD FEDERATION TECHNOLOGIES

Some of the technologies that provide mechanisms to support Cloud services are even provides federated cloud environment. Open Nebula provides an open-source and extensible architecture that can be modified to fit an individual Cloud. It can be leveraged by adding APIs and plug-ins to the existing architecture in order to facilitate inter-Cloud communication at different layers of the service stack. Eucalyptus is also an open-source framework that uses storage and computational infrastructure to provide a Cloud computing platform. Eucalyptus provides a modular, extensible framework with an Amazon EC2 compatible interface which can be utilized for federation at the IaaS layer.

Aneka Coordinator [R.Buyya] is a resource management and resource discovery tool used in an Aneka Enterprise Cloud to communicate and share resources with other Aneka sites which facilitates resource sharing and load balancing among the distributed Aneka Enterprise Clouds thus providing a decentralized IaaS federation. CometCloud is an autonomic computing engine that enables the dynamic and on-demand federation of Clouds as well as the deployment and execution of applications on these federated environments. It supports heterogeneous and dynamic Cloud infrastructures, enabling the integration of public/private Clouds and autonomic Cloud bursts, i.e., dynamic scale-out to Clouds to address dynamic workloads[16].

V. ISSUES IN FEDERATED CLOUDS

In Federated Cloud environments securing applications, services at different cloud stack layers due to cyber-attacks is complicated as federation involves complexity,

heterogeneity, and dynamic systems. Federated clouds pose challenges like whether the client or other cloud is servicing according to SLA agreements. The diversity and flexibility of the capabilities envisioned by Inter-cloud enabled federated Cloud computing model, combined with the magnitudes and uncertainties of its components, pose difficult problems and challenges in effective provisioning and delivery of application services in an efficient and secured manner [11]. Other issues related to configuring, Interoperability, Sharing ,Replication of data are some of the issues to be seriously addressed in future research work.

VI. CONCLUSIONS AND FUTURE STUDY

In this paper cloud computing and federation of cloud is studied briefly along with different architectures and issues. In case of federation cloud, the computing environment are heterogeneous, locations, Cloud service providers will use different protocols various measures, different Intrusion detection systems, security techniques for security will be used with different designs, interaction with clouds, sharing will become an issue. These issues should be studied deeply for better solutions in future research work.

REFERENCES

- [1] National Institute of Standards and Technology special publication.no.800-145, "The NIST definition of cloud computing" Sept. 2011
- [2] Cloud computing. Wikipedia. [online]. Available at http://en.wikipedia.org/wiki/Cloud_computing.
- [3] Cloud Computing Use Cases, A white paper produced by the Cloud Computing Use Case Discussion Group, Version 4.0 [online].Available. <http://cloudusecases.org>. July 2010,
- [4] Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", ICA3PP,2010,Part I, LNCS 6081, Springer, 2010 , pp. 13–31. doi: 10.1007/978-3-642-13119-6_2
- [5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2011), pp. 1-11. doi: 10.1016/j.jnca. 2010.07.006
- [6] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", V2.1, 2009.
- [7] Federated identity management", [Online], [Available],http://en.wikipedia.org/wiki/Federated_identity_management ,Dec, 2011,"
- [8] Xiao Zhang; Hong-tao Du; Jian-quan Chen; Yi Lin; Lei-jie Zeng, "Ensure Data Security in Cloud Storage", Network Computing and Information Security (NCIS), International Conference (IEEE), vol.1,14-15 May,2011 pp.284- 287. doi: 10.1109/NCIS.2011.64
- [9] Tobias Kurze_, Markus Klemsy, David Bermbachy, Alexander Lenkz, Stefan Taiy and Marcel Kunze," Cloud Federation", IEEE Computer society
- [10] M. A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii, International Conference on System Sciences (HICSS),2011,pp 1-9. doi: 10.1109/HICSS.2011.478
- [11] David Bernstein, Deepak Vij, "Intercloud Security Considerations" , 2nd IEEE International Conference on Cloud Computing Technology and Science, doi: 10.1109/CloudCom.2010.82. doi: 10.1109/ CloudCom. 2010.82

- [12]. Eghbal Ghazizadeh, Jamalul-lail Ab Manan et.al. *A Survey on Security Issues of Federated Identity in the Cloud Computing*, 2012 IEEE 4th International Conference on Cloud Computing Technology and Science, 2012. IEEE.
- [13] Paul Watson, *Application Security through Federated Clouds*, IEEE Cloud computing, 2014.
- [14]. K.Venkataramana, Prof M. Padmavathamma, "Threshold Secure Data Sharing Scheme for Federated Clouds", International Journal of Research in Computer Science eISSN 2249-8265 **Volume 2 Issue 5 (2012) pp. 21-28**
- [15] Attila Kertesz, Gabor Kecskemeti, Zsolt Nemeth, Marc Oriol, Xavier Franch, "A Holistic Service Provisioning Solution for Federated Cloud Infrastructures", S-Cube 2012, Zurich, Switzerland, IEEE
- [16] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I.M. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Cáceres, M. Ben-Yehuda, W. Emmerich, F. Galán, "The reservoir model and architecture for open federated cloud computing", IBM J. Res. Develop. 53 (2009) 535–545.
- [17] Sakshi kathuria, "A Survey on Security Provided by Multi-Clouds in Cloud Computing," International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.1, pp.23-27, 2018
- [18] Anitya Kumar Gupta, Srishti Gupta, "Security Issues in Big Data with Cloud Computing," International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.6, pp.27-32, 2017
- [19] Shaik. Munwar, K. Ramani, K. Madhavi, "Secure Data Storage Scheme using Blockchain for Federated cloud", International Journal of Computer Sciences and Engineering, Vol.07, Issue.06, pp.51-55, 2019

Authors Profile



Mrs.V.Keerthi pursued Master of Computer Science from Sri Venkateswara University, Tirupathi and Master of Philosophy in Computer Science from Dravidian University, Kuppam in 2017. She is currently pursuing Ph.D. in Dravidian University, Kuppam. Her main research work focuses on Cryptography Algorithms, Cloud Security and Privacy She is having 4 years of teaching experience.



Dr.T.Anuradha is working as a professor in the department of Computer Science and Dean, School of Science and Technology Dravidian University, Kuppam. She did her Ph.D. from Sri Padmavathi Mahila University in Tirupathi. She has 23 years of teaching experience. Her research areas are Data Mining & data warehousing, Neural Networks, Cloud Computing, Wireless Sensor Networks. She has published good number of journals in the same areas.
