International Journal of Soft Computing 12 (1): 1-6, 2017
ISSN: 1816-9503

A Survey on Federation of Cloud Computing and Supporting Protocols

[1]Chinthagunta Mukundha and [2]I. Surya Prabha
[1]Department of IT, Sreenidhi Institute of Science and Technology, Hyderabad, 501301 Telangana, India
[2]Department of IT, Institute of Aeronautical Engineering, Hyderabad, 500043 Telangana, India

Abstract: Cloud computing is a new emerging model to provide services to the customers. In the market there are more number of cloud vendors to provide cloud resources to the users. To organize all these cloud vendors we need some common standards and protocols. The main aim of research in the field of cloud computing federation is to achieve Quality of Service (QoS), cost efficiency and reliability cost efficiency by interconnected clouds and using federation concept among them.

Key words: Cloud computing, vendor, standards, protocols, efficiency, reliability

INTRODUCTION

The cloud computing paradigm advocates centralized control over resources in interconnected data centers under the administration of a single service provider. This approach offers economic benefits due to supply-side economies of scale, reduced variance in utilization of resources by demand aggregation as well as reduced IT management cost per user due to multi-tenancy architecture.

These benefits have contributed to the increasing industry acceptance of cloud services which are seen as more affordable and reliable alternatives compared to traditional in house IT systems and services. However, lower sides of the cloud computing paradigm are surfacing surveys show that potential customers hesitate to outsource their business applications and data into the cloud. Besides security concerns, application users are afraid of losing ownership and control. The lack of Standardized protocols, data formats and service interfaces is a portent of vendor lock-in (Armbrust *et al*., 2009). This problem can lead to underinvestment, an economically inefficient situation and therefore deserves our attention.

Cloud computing brings a concept by which scaling was redefined to the business applications. Neha Mehrotra and Nitin Dangwal by implementing its three very basic but grate implementation models, cloud made enterprise application and even general applications too more accessible to its developers and the users. The applications now resided centrally with its access and resource needs handled by a much smarter entity, known as the cloud. In addition, the implementation models too were very neatly designed, so as to adapt any application need which could be categorized easily amongst the business continuity, compliance or security domain.

Advantage of cloud federation (Grozev and Buyya, 2014)
Cost-effectiveness: Clouds with federation provide a larger amount of resources which may help improve cost-effectiveness. This include refinement for both the user and the provider such as for a given cost, reducing the time to completion, increasing the system optimizing or throughput the resource utilization.

Under-utilized: As the data center cannot be goes down, a cloud can decide to provide resources to other clouds when it realizes that its data center is under-utilized at given times. Typically, data centers are less utilized during the night and over-utilized during the morning. And this is varies from geographic area to other.

Diverse geographical locations: Most important that cloud service providers have to setup data centers worldwide. However, it is not possible that any provider will be able to setup datacenters in throughout the world.

Avoidance of vendor lock-in: By using multiple clouds and being able to freely transit workload among them, a cloud user can easily avoid vendor lock-in. In case a provider changes a policy or pricing that impact unfavorable its clients, client could easily migrate elsewhere.

Better SLA to customers: A cloud provider can provide better Service Level Agreements (SLA) to users as the result of competitive.

Corresponding Author: Chinthagunta Mukundha, Department of IT, Sreenidhi Institute of Science and Technology, Hyderabad, 501301 Telangana, India

Guaranteed performance: Due to limited resources that are available with a single cloud service provider, sudden increase in workload may lead to decrease of performance. Cloud federation is facing this disadvantage by renting resources from foreign cloud service stations, there by guaranteeing the agreed QoS.

Guaranteed availability: During unexpected disasters, the cloud system will be able to restore the services by federating with other cloud service providers in unaffected areas.

Literature review

Service models: Cloud computing distinguishes the service models Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS offers infrastructure services such as compute clouds, cloud storage, message queues, etc. PaaS offers complete platforms, solution stacks and execution environments while SaaS is a software delivery model driven by a multi-tenancy architecture.

Software as a Service (SaaS): The consumer uses an application but does not control the operating system, hardware or network infrastructure on which it's running.

The SaaS model dictates that the provider manages the entire suite of applications delivered to end-users. There fore SaaS providers are mainly responsible for securing these applications. Customers are normally responsible for operational security processes. However, the following questions, along with other sections within this document, should assist in assessing their offerings:

- What administration controls are provided and can these is used to assign read and write privileges to other users?

Platform as a Service (PaaS): The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework. Generally speaking, PaaS service providers are responsible for the security of the platform software stack and the recommendations throughout this document are a good foundation for ensuring a PaaS provider has considered security principles when de-signing and managing their PaaS platform. It is often difficult to obtain detailed information from PaaS providers on exactly how they secure their platforms however the following questions, along with other sections within this document should be of assistance in assessing their offerings:

- Request information on how multi-tenanted applications are isolated from each other a high level description of containment and isolation measures is required
- Is the SaaS access control fine grained and can it be customized to ones organizations policy?
- What assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?
- The platform architecture should be classic "sandbox" does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?
- PaaS providers should be able to offer a set of security features (reusable amongst their clients) do these include user authentication, single sign on, authorization and SSL/TLS

Infrastructure as a Service (IaaS): The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers but not the cloud infrastructure beneath them. As with personnel security, many of the potential issues arise because the IT infrastructure is under the control of a third party like traditional outsourcing, the effect of a physical security breach can have an impact on multiple customers:

- What assurance can you provide to the customer regarding the physical security of the location? Please provide examples and any standards that are adhered to, e.g., Section 9 of ISO 27001/2
- Who, other than authorized IT personnel has unescorted access to IT infrastructure?
- For example, cleaners, managers, "physical security" staff, contractors, consultants, vendors, etc.
- How often are access rights reviewed?

MATERIALS AND METHODS

Deployment models

Public cloud: In simple terms, public cloud services are characterized as being available to clients from a third party service provider via. the internet. The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

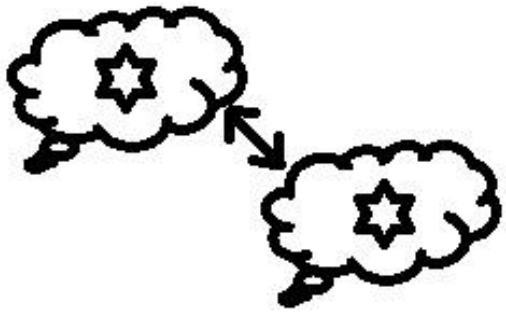

Fig. 1: Homogeneous cloud federation

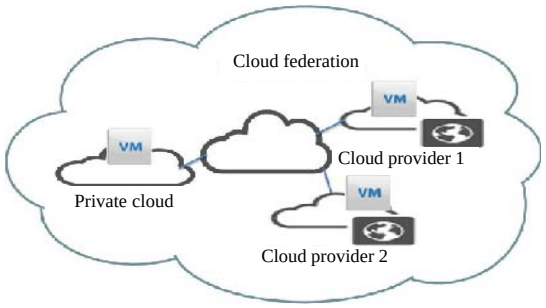

Fig. 2: Heterogeneous cloud federation

Private cloud: A private cloud offers many of the benefits of a public cloud computing environment such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infra-structure, improving security and resiliency because user access and the networks used are restricted and designated.

Community cloud: A community cloud is controlled and used by a group of organizations that have shared interests such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

Hybrid cloud: A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non-business-critical information and processing to the public cloud while keeping business-critical services and data in their control (Aversa *et al*., 2011).

Approaches to cloud federation

Homogeneous cloud federation: The simplest of approaches, according to which one cloud would be federated to another by the service vendor whereby the participating enterprise would have no knowledge of it. And that is because, the enterprise is not responsible for the addition and migration of infrastructure related to its service. It's the service vendor himself responsible for its management shown in Fig. 1.

Heterogeneous cloud federation: An elongation of the homogeneous federation but with a facility to federate a public cloud with a private cloud. However, it should be noted that a public cloud cannot be federated to a private cloud but a private cloud can be federated to a public cloud. This federation here talked about is in relevance to the access, i.e., private cloud can access a public cloud but a public cloud cannot access a private one (Fig. 2).

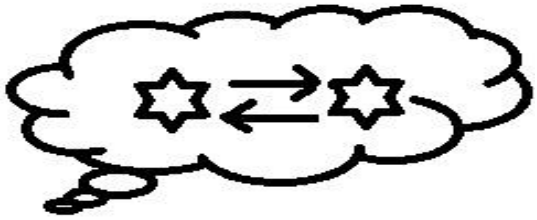

Fig. 3: Federation among applications on the same cloud

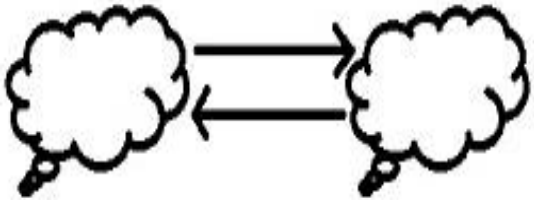

Fig. 4: Federation among applications on different clouds

Federation among applications on the same cloud: There may be applications that link to one another at a point of time. Mostly transactional applications fall into this category. It may happen that products may be displayed at a different service, they may be transacted at a different one and their payment may be performed by a different one. In addition, some centralized services also exist, like the one we have in Google providing a single sign-on to its each and every service shown in Fig. 3. When these altogether different services reside on the same cloud, they can be federated to a single sign-on and better user experience.

Federation among applications on different clouds: Very similar to the federation discussed above. But, the difference here would be that the applications would now be residing over different clouds and they would be federated (Fig. 4).

Interoperability between services providers: When an application is being designed, it is obvious that it will use any machine specific cloud library for its implementation and deployment. Moreover, by federating, the freedom a service vendor gets is to attach an application to any desirable service provider, i.e., a cloud. However, it should be noted that the implementation of the virtual machine that exists on that particular cloud which is being federated might be different from the one in which the application had been actually designed. Thus, the need arises for interoperability.

What interoperability offers is a very clean application migration from one service provider to another. The application undergoes some very simple reconfiguration processes and no need exists to re-design the application for any target machine implementation due migration.

RESULTS AND DISCUSSION

Cloud federation: Cloud federation compose services from different providers aggregated in a single pool supporting three basic interoperability features resource transfer, resource redundancy and combination of complementary resources resp. services. Migration allows the moving of resources such as data items, virtual machine images, source code, etc. from one service domain to another domain. While redundancy allows concurrent usage of similar service features in different domains, combination of complementary resources and services allows merging of different types to aggregated services. Service disaggregation is nearly linked to cloud federation as federation eases and advocates the modularization of services in order to provide a more efficient and flexible overall system. We identify two basic dimensions of cloud federation: horizontal and vertical. While federation of horizontal takes place on one level of the cloud stack, e.g., the application stack, vertical federation spans multiple levels.

Several aspects of horizontal federation can be distinguished, e.g., geography and provider domain. Horizontal federation across provider domains may decrease provider dependency and thereby lower the risks of vendor lock-in and hold-up. Improving availability may be achieved through horizontal federation across multiple geographic regions. Also, federation of vertical scenarios along similar aspects are imaginable. Cloud federation can be of interest for providers as well as for users. Customers may profit from lower costs and better performance while providers may offer more sophisticated services.

Buyya *et al.* (2010) mentioned that the cloud computing providers have more data centers at different geographical locations over the internet in order to serve needs of their customers around the world. However, current systems do not support mechanisms and policies for dynamically coordinating load distribution among different cloud in order to determine optimal location for hosting application services to achieve QoS levels. The key elements for enabling federation of clouds are: cloud coordinators, brokers and cloud exchange.

Carlini *et al.* (2011) contrail is an open source and integrated approach that are designed to combine a number of independent cloud in to one integrated federated cloud which aims offering (IaaS) infrastructure as a service and (ConPaaS) contrail platform as a service. User can submitted work to the cloud federation and let the federation to select the best resource provider for execution. Contrail is built around a centralized entity and works based on the broker services (federation support) that act as mediators between cloud users and cloud providers.

Rochwerger *et al.* (2009) cloud at home. The idea behind cloud at home that computing resources of single users accessing the cloud can be shared with the others. This new computing paradigm gives back the power and the control to customers who can decide how to organize their resources/services in a global, geographically distributed context. They can voluntarily scientific projects by providing their resources to scientific research centers for free or they can earn money by trading their resources to cloud computing providers in a pay per use/share context. Cloud@Home users voluntarily share their resources without any problem. The scenario authors are composed of several coexisting and interoperable clouds. Open clouds identify open VO (Virtual Organization) for free volunteer computing; commercial clouds identify companies selling their computing resources to earn money; hybrid clouds can both sell or give for free their services. Both open and hybrid clouds can operate with any other clouds. In this way it is possible to make federations of clouds working together on the same project. This can take users to choose the best provider that matches their requirements in easy way. Cloud providers can establish business relationships, agreements and strategies to achieve the best market performance, reducing costs and maximizing revenues.

Ranjan *et al.* (2013) to create scalable wide-area networking of compute elements, researchers describes Aneka-Federation, a decentralized and distributed system that combines enterprise clouds and structured

peer-to-peer techniques. Researchers have two objectives the first is to design and development of scalable, decentralized, self-organizing and federated cloud computing system. The second is to introduce the Aneka-Federation is a software system that incorporates various software services, peer-to-peer resource discovery protocols and resource provisioning methods to deal with the challenges in designing decentralized resource management system.

Celesti *et al.* (2010), the researchers define three subsequent stages of cloud computing services in the term of federation: Stage 1 "monolithic" (now), cloud services depends on independent proprietary architectures Stage 2 "vertical supply chain", cloud providers will request cloud services from another providers Stage 3 "horizontal federation", smaller, medium and large cloud providers will federate themselves. Currently, the major clouds are planning to the Stage 2.

Researchers describe how to implement heterogeneous cloud surrondings in Stage 3 "horizontal federation" where clouds can work together and providing new business opportunities such as cost-effective, power saving and on demand resources provisioning. Researchers propose a solution based on the Cross-Cloud Federation Manager (CCFM) which is a new component inside the cloud architectures, allowing a cloud to establish the federation with other clouds. In cross-cloud federation model where the federation establishment, between a cloud needed external resources and a cloud provided resources, passes through three main phases discovery, match-making and authentication.

Rochwerger *et al.* (2009) European project focusing on cloud federation is reservoir the resources and services virtualization, the researchers define a reservoir cloud as decentralized federation of collaborating sites. Its architecture does not feature a central entity and is peer-to-peer-clouds communicate directly with each other. In the reservoir model there is a clear separation between the functional roles of service providers and infrastructure providers.

Goiri researchers present a complete characterization of providers? federation in the cloud including decision equations to outsource resources to other providers, rent free resources to other providers or shutdown unused nodes to save power and characterize these decisions as a function of several parameters then authors evaluation how a provider can enhance its profit by using these equations to develop federation. The authors approach is based on a global scheduler deployed on each cloud. That is responsible for allocated resources for all the VMs running in that provider. This includes both the movements among the different nodes in that provider and between that provider and other federated cloud providers. For saving power consumption of the provider the scheduler can shut down nodes that remain unused in order to reduce power consumption in the provider.

Federation challenges

Autonomics: System management becomes too complex to be carried out only with human intervention and manual administration in cloud federation. So, to overcome this issue, we need for autonomics computing. Autonomic computing means self managing of computer-based systems while hiding the complexity of the system. Using techniques provided by autonomic computing, we can handle different system requirements such as performance, fault tolerance, reliability, security, QoS, without manual intervention. Autonomic management tasks including self-configuration (i.e., automatic configuration of components), self-healing (i.e., automatic discovery and correction of faults), self-optimization (i.e., automatic optimization of resource allocation) and self-protecting (i.e., automatic system security and integrity).

Interoperability: In cloud federation each cloud comes with its own solution and interfaces for services (Amazon, Microsoft, Google and Sales Force). In a heterogeneous cloud federation scenario, interoperability is a key concept. Current cloud computing offerings usually "lock" customers into a single cloud infrastructure, platform, or application, preventing the portability of data or software created by them. create standard interfaces that will enable interaction between distributed sites, allowing the federation of infrastructures issues must be taken into account when platform for interoperability among different cloud vendors is create.

Security: In federated clouds each cloud could use different Authentication and Identity Management (IdM) this is first issue to be overcome, in order to perform authentication among heterogeneous clouds. Effective identity management in inter-cloud environments requires support for established standards such as X.509 certificates SAML and WS-Federation (Bernstein and Vij, 2010).

Service-Level Agreement (SLA): In federated cloud environments each participant cloud provider has its own SLA management mechanisms. We need to set up a global SLA. By global SLA, we mean comprehensive SLAs between the user and the federation including all SLAs for each cloud provider.

Federation protocols

Security Assertion Markup Language (SAML): SAML is generally used in business deals for secure

communication between online partners. It is an XML based protocol used for authentication, authorization among the partners. SAML defines three roles: the customer, a Service Provider (SP) and an Identity Provider (IDP) (Armbrust *et al*., 2009). SAML provides queries and responses to specify customer attributes authorization and authentication information in XML format. The requesting party is an online web portal that receives security information.

Open Authentication (Oauth): It is a method used for interacting with protected data. It is basically used to provide information access to developers. Users can grant access to information to developers and consumers without sharing of their identity. OAuth does not provide any security by itself in fact it depends on other protocols like SSL to give security.

OpenID: OpenID is a Single-Sign-On (SSO) method. It is a common login process that allows customer to login once and then use all the participating systems. It does not based on central authorization for authentication of customers.

SSL/TLS: TLS is used to provide secure communication over TCP/IP. TLS generally implemented in three phases: in first phase, negotiation is done between clients to identify which ciphers are used. In second phase, key interchange algorithm is used for authentication. These key exchange algorithms are public key algorithm. The third phase involves message encryption and cipher encryption.

CONCLUSION

This study presents all available different federation rules to organize the cloud and the protocols need to communicate different cloud environment.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph and R.H. Katz *et al*., 2009. Above the clouds: A Berkeley view of cloud. Technical Report No. UCB/EECS-2009-8. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Aversa, R., M. Avvenuti, A. Cuomo, B. Di Martino and G. Di Modica *et al*., 2011. The Cloud@Home Project: Towards a New Enhanced Computing Paradigm. In: Euro-Par 2010 Parallel Processing Workshops, Guarracino, M.R., F. Vivien, J.L. Traff, M. Cannatoro and M. Danelutto *et al*. (Eds.). Springer, New York, ISBN-13: 9783642218781, pp: 555-562.

Bernstein, D. and D. Vij, 2010. Intercloud security considerations. Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom), November 30-December 3, 2010, IEEE, New York, USA., ISBN:978-1-4244-9405-7, pp: 537-544.

Buyya, R., R. Ranjan and R.N. Calheiros, 2010. InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services. Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing, May 21-23, 2010, Busan, South Korea, pp: 13-31.

Carlini, E., M. Coppola, P. Dazzi, L. Ricci and G. Righetti, 2011. Cloud federations in contrail. Proceedings of the European Conference on Parallel Processing, August 29-September 2, 2011, Springer, Berlin, Germany, pp: 159-168.

Celesti, A., F. Tusa, M. Villari and A. Puliafito, 2010. How to enhance cloud architectures to enable cross-federation. Procededings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), July 5-10, 2010, IEEE, Messina, Italy, ISBN:978-1-4244-8207-8, pp: 337-345.

Grozev, N. and R. Buyya, 2014. Inter-cloud architectures and application brokering: Taxonomy and survey. Software Pract. Experience, 44: 369-390.

Ranjan, R., R. Buyya and S. Nepal, 2013. Editorial: Model-driven provisioning of application services in hybrid computing environments. Future Gener. Comput. Syst., 29: 1211-1215.

Rochwerger, B., D. Breitgand, E. Levy, A. Galis and K. Nagin *et al*., 2009. The reservoir model and architecture for open federated cloud computing. IBM. J. Res. Dev., 53: 4-11.