International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 23 (2015) pp 43373-43377
© Research India Publications. http://www.ripublication.com

Ontology in Cloud Computing: A Survey

N. Geetha

Research Scholar Department of Computer Science and Engineering Pondicherry Engineering College Puducherry.
E-Mail:great. geetha@gmail. com

Dr. M. S. Anbarasi

Assistant Professor Department of Information Technology Pondicherry Engineering College Puducherry.
E-Mail:anbarasims@pec. edu

Abstract

Today Cloud Computing has gained its place in almost every area of technology through its great features like on demand self service, elasticity and resource pooling. Besides these features, the cloud computing doesn’t provide a unique semantic ground like that of semantic web. To overcome these shortages of cloud and to provide an environment that could enable searching of service and resource automatically, ontology could be used. Ontology can enhance dynamic discovery of services across various cloud computing environments, could provide an intelligent framework for Software as a service and many more. This paper makes a clear survey on the use of ontology in various areas of cloud computing like maintaining Resource Catalogues, managing SAAS infrastructure, security etc.,.

Keywords: Cloud Computing, Dynamic service Discovery, Ontology.

I. INTRODUCTION

Cloud Computing has become a paradigm for provisioning software, infrastructure and platform as a service. There are several benefits of cloud including flexibility and pay as per use. According to Linthium[1] “Cloud Computing is a pay per use model for enabling available, convenient, on demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Cloud computing is a model that enables ubiquitous, convenient on demand network access to many users where the users need not own the infrastructure for computing service. The property of scalability and multi-tenancy can be improved greatly. The deployment, allocation and reallocation of resources thus become easier [2]. According to Tharam Dillon et al [3] cloud computing are evidently articulated as:-

On-demand self-service:

Consumers who need resource for a limited period of time can easily gain that service automatically. The resources include CPU time, Storage on network, software and so on.

Broad network access:

Customers can also demand for network as a part of service. These computing resources are delivered to the customers over the network. They are then used by a variety of client application platform according to their suite.

Resource pooling:

The computing resources are pooled together to serve the consumers who are using either a multi-tenancy or virtualization model. These virtual and physical resources are dynamically assigned and reassigned according to the customers demand. The main goal of such pool based computing platforms is economy and specialization [4]. In such a scenario the customers will not have a full control or knowledge about the location of the resource and their originalities.

Rapid Elasticity:

In cloud, the resources for the customers are not persistent. They are given to the user immediately when a request arrives. It is not an upfront contract that the users must use them and release them when they complete their work. The resources that are provisioned to them are infinite in nature. In the demand of the consumers, the resources are generated and provided by the cloud providers.

Ontology on the other hand, represents knowledge as a set of concepts in a particular domain. The main use of ontology is to organize information. It conceptualizes a domain. It includes machine understandable definitions of the concepts in the domain for sharing common understanding of structure, separating domain knowledge from that of operational knowledge and analysis of domain knowledge and reasoning. Several research works have been carried out in the field of ontology incent years. The most recent development for the web is the emergence of services providing libraries for specific domains. These libraries are called Ontology library. Providing security and privacy in cloud is the major issue in cloud computing [5]. This is also being reduced using ontology. The following sessions of discussion will give a more clear idea on the use of ontology in various areas of cloud computing.

II. ONTOLOGY IN CLOUD COMPUTING

A. Inter-Cloud Directories and Exchanges using Ontology.

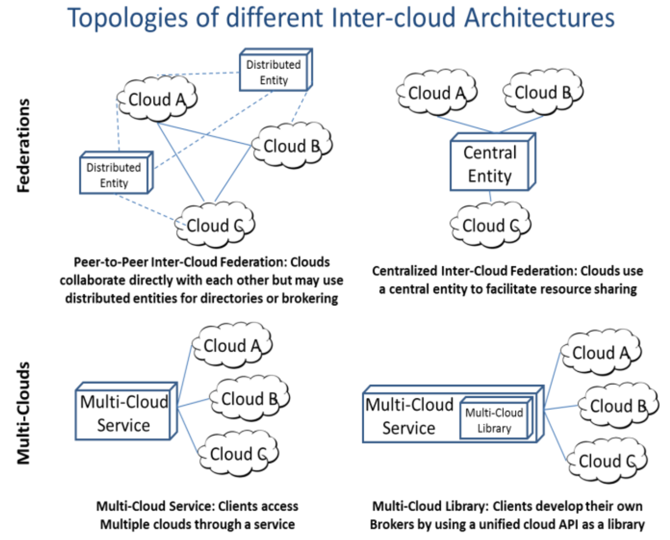
There are numerous services that are provided by separate cloud providers. The exchange of data and resources among these separate clouds may be challenging. Hence the Inter

Cloud Directories provide an effective connectivity and collaboration between separate clouds. In this mechanism, there is a cloud catalog which uses ontology to automate the environment by which the software agents can discover the services and consume those services.

Inter-cloud Topology

Services in cloud are provided by different cloud service providers. Each cloud provider has a different and own topology of network. Intercloud topology aims at interconnecting multiple cloud provider's infrastructure. The interconnection of these cloud service providers can be done only to a certain extent. In the intercloud topology each cloud service provider is called a cloud instance. Each cloud instance should have the capability of interacting with each other. Each cloud should be able to find out other cloud in existence. Another issue that arises in the intercloud topology is the problem of interoperability. To overcome these issues, an Intercloud Protocol is set to support 1-to-1 and many-to-many communication service.

The different topology that exists is a) Peer-to-peer intercloud. b) Centralized intercloud c) Multicloud services and d)Multicloud library. Fig. 1 illustrates the above said architectures. When different clouds share their services, the process of brokering is also needed. Brokers come as a part of service that provides access to the set of clouds.



Peer-to-Peer Inter-Cloud Federation: Clouds collaborate directly with each other but may use distributed entities for directories or brokering

Centralized Inter-Cloud Federation: Clouds use a central entity to facilitate resource sharing

Multi-Cloud Service: Clients access Multiple clouds through a service

Multi-Cloud Library: Clients develop their own Brokers by using a unified cloud API as a library

Fig: 1 Inter-Cloud Architecture

B. Ontology based Cloud Computing Recourse Catalog

Cloud is bundled with many resources which are provided by several different cloud providers. In order to fulfill a business goal and need, many resources have to be integrated. These resources have to be managed in a very efficient way which requires a proper planning to fulfill the needs. The most popular way of managing this is the use of UDDI which is in practice. UDDI maintains a Taxonomy based catalog. Taxonomy has a class/subclass relationship which is not sufficient to maintain a larger class of resource. Hence for a better solution, Ontology is applied to reduce the domain complexity.

C. Ontology based framework for intelligent customization of Software as a Service.

Multi tenancy architecture of cloud providers provides a facility for the users to share the software with appropriate customization. Cloud consumers release their applications on a hosting environment, which can be accessed through networks from various clients (e. g. web browser, PDA, etc.) and application users. Cloud consumers do not have control over the Cloud infrastructure that often employs multi-tenancy system architecture. Different cloud consumers' applications are organized in a single logical environment on the SaaS cloud to achieve a good scale of economy and optimization in terms of speed, security, availability, disaster recovery, and maintenance. Han and Sim [6] presented a Cloud service discovery system that uses Cloud ontology to determine the similarities between and among services. This system is based on Agents which enables the reasoning of relations among services. The cloud ontology specified here consists of the concept of searching the cloud services more efficiently.

Software as a Service(SaaS) is a multi tenancy architecture where the software is developed by the software providers who publish their copy of their software on the web for multiple users. This architecture enables the user to customize their GUI, Data and User interactions. The SaaS customization has to meet various goals. The service providers who provide Software as a Service have to support tenants/ customers with a huge number of options and variations such that it is possible for each tenant to have a unique software configuration by using a single code. They must also ensure that the configuration must be so easy and simple that the user need not build an extra equipment to use the software being provided. This customization is the base for the QoS aspect of cloud [7]. A fully customizable SaaS application has a layered architecture.

The framework has several layers in which the data layer, service layer, Business Process layer and User Interface layer are the major ones. The data layer holds the ontology descriptions for particular domains. This ontology is specified by different communities. These are organized in the form of a tree. The conceptual similarity is matched between ontology of various communities. When a match is found, the value is set to 1. A template is then found after matching the domain ontology for customization. These are then updated in the database for future reference.

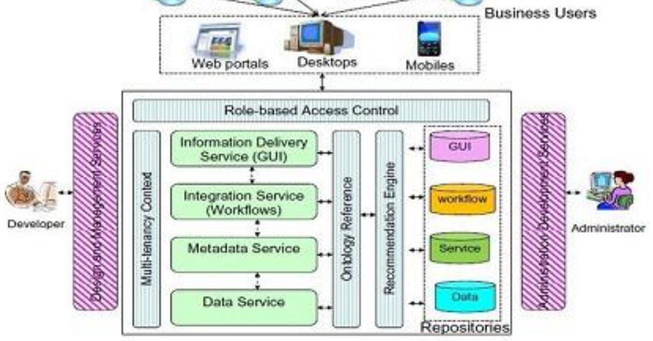


Fig:2. Layered Architecture

D. Design of security system

Security is one of the major challenges faced by all cloud infrastructures. Since the cloud is multi tenancy architecture, data in the cloud has a greater chance to get lost, be computed and modified by several service users. Data integrity, recovery and privacy are another issue that has to be managed properly in cloud environment. As an example scenario, if software is being modified by any company or organization, it might affect the other service users of the same software. This might cause a drastic effect in other firm in terms of data. The data may also be modified by the administrators. Hence proper and efficient management of data and security has to be given to cloud infrastructure. In order to restrict the users modifying the data, many kinds of access control mechanism is proposed namely User Based Access Control, Discretionary access Control, Mandatory Access Control and Role Based Access Control. The following session focuses on the discussion of some of the access control mechanism in use.

Discretionary Access Control

This is a very traditional access control mechanism where access is given to the user according to the user identity and authorization which is defined for open policies. DAC holds the permission to particular user to particular objects. DAC is a mechanism of "who can access what". The access list is associated with each object's file system [8]. In this mechanism, the owner of the object can give access rights and permission to other users.

Mandatory Access Control

In mandatory access control mechanism, Security levels are provided. This works with the principle of access to objects to the number of subjects. Individuals do not have access to change the access. MAC is a Read down and Write up mechanism [9]. In this method, users can be associated with the objects based on the degree of trust and security levels given to them. It is been found after many researches that MAC are more powerful than DAC.

Role Based Access Control.

Though cloud is multi tenancy architecture, not all users are given equal rights. To give higher level of security to data and the cloud services, a new approach called Role Based Access Control is followed. The access of software or a service is provided to the cloud users according to their roles and responsibilities within the cloud environment. Roles represent specific functions within the organization. There are studies being done using security tags in BCP model [10]. A Role Based Access Control system has two phases. Phase one deal with the user with one or more roles. Phase two checks the roles against requested operations. The roles can be dynamically assigned and reassigned or can also be removed. This will not change the permission associated with the roles. Roles are the functions that a particular user performs on a particular domain or organization. Roles can be represented by a hierarchical structure that represents organization's line of authority and responsibility. The roles of the juniors lie at the bottom and those of the seniors lie at the top of the hierarchical role diagram

IV BENEFITS OFROLE BASED ACCESS CONTROL

Define Roles with Semantic Information:

Every domain has its own semantics. According to the semantics of a particular domain the roles are assigned to them along with their position and their job functions. For an IT company, the roles may be CEO, CFO, Manager Etc., Functions are the daily duties of an individual according to their roles. Each role has different access control mechanism to work on the data and the resources. Each employee can be assigned with multiple roles.

Manage Roles Hierarchy with Ontology:

In a larger domain, there may be several roles. In order to define and differentiate the roles a clear ontology is requires. The roles of different domains may be same but their functions may differ. For example, ACM and IEEE are two large communities. They have their own standards and practices, and they are similar but distinct. To solve these heterogeneities, a large and complete ontology are built at a higher level by which the roles and their functions can be distinguished. Each role can be defined properly and efficiently.

Role Hierarchy:

Ontology for a role hierarchy may be formed and represented in the form of a tree. An unordered and labeled ontology tree is a Tuple OT = (V, E) where V is a finite set of nodes, E is a set of edges connecting the edges where $E \subset V X V$, representing the relationship between nodes. If $(u, v) \in E$, u is the parent of v, denoted as u=parent (v) and v is the child of u, denoted as v=child (u).

Role Numbers and ensure Scalability:

The total number of possible roles may be the product of every category and its dimension. The number roles can hence be the subset of the combinations of roles of different dimension and category.

Reference Ontology Framework for Role Based Access Control

The reference Ontology framework for role based access control consists of five major components.

Tenant:

Tenant is a user or any human in the cloud who is involved in the web of cloud.

Role:

Role is said to be the Job function within an organization. Role describes the responsibility of a particular user within the organization and classified according to the security requirements of the system.

Permission:

It is the permission granted to a particular mode of access to one or more tenants. It is the authorization, access rights and privilege given to one or more tenants in the organization.

C**onstraints**:
Constraints are the security condition for a particular action. These constraints are applied to a role. When these constraints are applied to a role, it returns a value for the acceptance or rejection of the constraints.

Sessions:
The roles of the users are activated for a session to perform the operations they are intended to. Each session maps one user to many roles as per specifications.

To build up a new security model for access control for a particular application in the cloud, it is not necessary to start from the scratch. For developing a new ontology for a domain, the Ontology DB can be searched for that particular domain. The module called the Reference Ontology provides a list of candidate ontology template. The new template is derived from the existing one for the tenants to use. If the tenant has his own role architecture design, the template can be imported into the system. The component called the Ontology Comparator then compares the similarity of its own ontology with the other candidate ontology. The one most similar with the highest score can be reused. If the tenant doesn't have his own ontology well-defined, a default ontology template along with the policy template in his domain is provided for reference.
The contextual information from both environment and the tenants is collected by the Context Collector when a session is created. The Role Evaluator then uses this contextual information and interacts with the databases and policy databases to determine the security level, role and access policy. The Policy Controller grants, denies and revokes the access policy of a tenant in the cloud environment. The result of this security service is delivered to the service model and the operations are performed according to the security checking process.

V RESEARCH DIRECTION

There are several researches that are being carried out by several researchers on cloud using ontology. This paper gives some of the research directions that can be taken and enhanced. Besides application and software, firmware is also one of the layers of the Cloud Stack. Hence an Ontology model can be developed to facilitate the interoperation among different cloud systems [16]. In Mobile Cloud Computing, Ontology can be used to provide distributed IT resources and services to the users based on context aware information [17]. For Enterprise Cloud Management, Ontology can be used to capture information relevant to specific users and to integrate data from various data sources [18]. Alignment between Ontology in cloud computing architecture is also one of the major issues that can be addressed.

VI CONCLUSION

Cloud computing and Ontology are the two emerging fields where the researchers are doing many more activities to enhance their application. Ontology may be applied to any of the traditional and emerging area like Software Engineering, Data Mining and Information Engineering etc. This paper to some extent has given an overview of the use of Ontology in a very promising technology called the Cloud. This paper addresses the computing resources present across disparate clouds, the technique for protecting sensitive information from unauthorized access and improving the overall efficiency of Cloud.

VI REFERENCES

[1] D. S. Linthium, “Cloud Computing and SOA Convergence in your enterprise: a step-by-step guide”, 1st Edition, Addison Wessley, 2009.

[2]. Peter Mell, Tinothy Grane, “The NIST definition of cloud computing”, Jan 2011.

[3] Tharam Dillon, Chen Wu and Elizabeth Chang, “Cloud Computing issues and challenges”, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[4] [1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15, " *21. Aug 2009,* 2009.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing, " *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28,* 2009.

[6] Taekgyeon Han and Kwang Mong Sim, “An ontology-enhanced Service Discovery Systems” Proceeding of International Multi conference of Engineers and Computer Scientists, Vol 1, March 2010.

[7] www. CloudOntology. Wikispaces. asu. edu.

[8] K Punithasurya, S Jeba Priya, “Analysis of different Access Control Mechanism in Cloud”, International Journal of Applied Information System, 2012.

[9] R. Sandhu and P. Samarathi, “Access Control Principles and Practice”, Proceedings of 17th NIST-NCSC National Computer Security Conference, Baltimore MD. pp. 34–46.

[10] N. Kwak and C. Chong Ho, “ Input feature selection for classification Problems”, IEEE Transaction on Neural Networks, Vol 3, 2002.

[11] Parminder Singh and Sarpreet Singh, “Towards Novel and Efficient Architecture for Extended-RBAC in cloud computing”, International Journal of Computer Science and Information Technologies, Vol4(3), 2013

[12] D Nguyen, J Park, R Sandhu, “ A Provenance-Based Access Control Model for Dynamic Seperation of Duties” International Conference on Privacy, Security and Trust (PST), 2013 - ieeexplore. ieee. org.

[13] Bibin K Onankunju, “Access Control in Cloud Computing”, International Journal of Scientific Research and Publications, Volume 3, Issue 9, September 2013.

[14] Zhifeng Xiao and Yang Xiao, “ Security and Privacy in Cloud Computing”, IEEE Communicatiuons Survey and Tutorials, Vol 15. 2013.

[15] Kuyoro S. O, Lbikunle F, Awodele O, “Cloud Computing Security Issue and Challenges” International Journal of Computer Networks(IJCN), Volume(3): Isseue(5), 2011.

[16] L. Youseff, M. Butrico, D. D. Silva. “Toward a Unified Ontology of Cloud Computing”. In Proceedings of Grid Computing Environments Workshop, 2008.

[17] Changbok Jang, Euiin Choi. “Context Model Based on Ontology in Mobile Cloud Computing”. Communications in Computer and Information Science, Volume 199, 146-151, 2011.

[18] Peter Haase, Tobias M., Michael Schmidt, et al. “Semantic Technologies for Enterprise Cloud Management”. In Proceedings of the 9th International Semantic Web Conference, 2010.

[19] J. Bock, Alexander lenk, Carsten D.. “Ontology Alignment in the Cloud”. In Proceedings of ontology matchingworkshop2010.