ISSN:0975-9646

Collaboration in Multicloud Computing Environments: Framework and Security Issues

Madivalayya M Hiremath
Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore 560054, India

Dr. Annapurna P Patil
Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore 560054, India

Abstract*—Cloud computing has newly emerged as a new key knowledge for outsourcing organizations IT infrastructures on an economical source. It allows a lively provisioning of virtual hardware and scalable applications according to their requirements using a transparent easy "pay as you go" pricing model. The current flow in cloud computing arises from its capacity to provide software, infrastructure, and platform services without requiring large investments or expenses to manage and operate them. A planned proxy-based multicloud computing framework allows active, on-the-fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without preestablished collaboration agreements or standardized interfaces. planned work uses cloud hosted proxies to provide collaboration in multicloud computing environment where in each CSP (Cloud Service Providers) can host proxies within its cloud infrastructure, manage all proxies within its organizational domain, and handle service requests from clients that want to use those proxies for collaboration.

Keywords*—multicloud, proxy, mashups, collaboration, cloud service provider.

I. INTRODUCTION

Cloud computing is the release of computing services over the Internet. Cloud services allow persons and businesses to use software and hardware that are managed by third parties at distant locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. Cloud computing characteristics include network-based access channel, resource pooling, multitenancy, automatic and elastic provisioning and metering of resource usage. High availability and scalability of resources can be done using technique named as virtualization.

Virtualization of resources such as processors, network, memory and storage helps user to progress increase performance, scalability and high availability. Clients can use these resources to host applications and even client can use to store their data. Rapid changes of resources demand can help to deal with variable demand and proving optimum resource utilization. As more organizations are using cloud computing, cloud service providers (CPSs) are developing new technologies to progress the cloud's capabilities. Now the term, mashups are a new trend. It means combining services from multiple clouds into a single service or application. This service composition makes cloud service providers (CSPs) to propose new functionalities to clients at lower development costs. Examples of cloud mashups and technologies are IBM's Mashup Center, Appirio Cloud Storage and Force.com for the Google App Engine. For example, cloud-based electronic medical record (EMR) management systems like [1] Practice Fusion, Verizon Health Information Exchange, Medscribbler, and GE Healthcare Centricity Advance are emerging.

Cloud mashups want pre-established agreements among providers as well as the use of custom built, proprietary tools that combine services through low-level, tightly controlled and constraining integration techniques. This approach to building new collaborative services does not support agility, flexibility, and openness [2]. Realizing multicloud collaboration's full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services reach across multiple clouds that lack pre established agreements and proprietary collaboration tools. While cloud standardization will support collaboration, there are number of hurdles to its adoption. From a market perspective, it is doubtful that multiple CSPs will agree on an easy and standardized way to access services, as this would give clients total freedom in changing providers, leading to increased open and direct competition with other providers. Cloud-based computing also introduces new security concerns that affect collaboration across multi cloud applications they are, increase in the attack surface due to system complexity, loss of client's control over resources and data due to asset

migration, threats that target exposed interfaces due to data storage in public domains, and data privacy concerns due to multitenancy [13]. So there is need of developing multi cloud system which provides trust, security and safety for applications and data. Keeping all these drawbacks my work is to develop a generic cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. There are restrictions in the current cloud computing model prevent direct collaboration among applications hosted by different clouds.

A method that could overcome these restrictions uses a network of proxies. A proxy is an edge-node-hosted software instance that a client or a CSP can delegate to carry out operations on its behalf. Proxies can act as mediators for collaboration among services on different clouds. As an example of proxy-facilitated collaboration between clouds, consider a case in which a client or CSP wishes to simultaneously use a collection of services that multiple clouds offer. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications [14]. A client or a CSP might employ multiple proxies to interact with multiple CSPs.

II. MOTIVATION

The main objective of cloud computing is to support agility, flexibility and openness. The "pay as you go" model is established through predefined Service Level Agreements (SLAs) that are custom-built. Proprietary tools and services are integrated to control and monitor such a service. Different companies provide different services on cloud. Bringing these different services together and creating mashups require pre established agreements among providers and dynamic SLA selection. Though SLAs are custom-built, there are many challenges that prevent direct collaboration of different cloud services hosted by different clouds. Secure collaboration of such services is the need for tomorrow which motivated to take up this project.

III. LITERATURE SURVEY AND RELATED WORK

A. Efficient proxy signatures based on trapdoor hash functions

Proxy signatures have create extensive use in authenticating agents performing on behalf of users in applications such as grid computing, communications systems, personal digital assistants, information management and e-commerce [3]. Proxy signature concept is very important aspect and has been highlighted by applied cryptographers through different variations, namely Threshold proxy signatures, blind proxy signatures and so forth. Unfortunately, construction of new proxy signatures provide minor or minimum weakness compared to previously developed schemes, and these do not deliver official security guarantees. In this study, so because of these drawbacks or constraints the authors propose a method called trapdoor hash functions to construct provably secure proxy signature schemes that can be used to authenticate and authorize agents acting on behalf of users in agent-based computing systems [2]. They show the effectiveness of their approach for creating realistic instances by constructing a discrete log-based instantiation of the proposed general technique that achieves better performance in terms of verification overhead and signature size compared with presented proxy signature schemes [5]. Formal definitions, security specifications and a detailed theoretical analysis, including correctness, security and performance, of the proposed proxy signature scheme have been provided.

B. SLA based service brokering in intercloud environments

Cloud computing is a fast growing technology and user has many options in choosing cloud infrastructure. Because of different and less interoperable cloud infrastructures, there are challenges and problem for cloud users when selecting appropriate cloud infrastructure and it makes users to continue with particular cloud provider [5]. So researches are going to adapt to a standards, now users can easily migrate from one cloud service provider to other. Intercloud is network of clouds connected through networks. This allows users to easily transfer their application workloads across Clouds despite of the underlying used Cloud provider platform [10]. A very talented future use case of Intercloud computing is Cloud services brokerage. In this paper, authors propose a generic architecture for a Cloud service broker operating in an Intercloud environment by using the latest Cloud standards. The broker aims to find the most appropriate Cloud provider while fulfilling the user's service requirements in terms of functional and non-functional Service Level Agreement (SLA) parameters [19]. After discussing the broker value-added services, authors present in detail the broker design. We focus especially on how the expected SLA management and resource interoperability functionalities are included in the broker.

C. Intercloud Security Considerations

Cloud computing is a new design example for large, distributed datacenters. In cloud computing users can store their data using cloud infrastructure and even they can access the applications like email, search, and social networks, Service providers offer These all services [7]. Newly authors have increased offering services to users like, compute related capabilities such as virtual machines, storage, and complete operating system services. The cloud computing design yields breakthroughs in geographical distribution, resource utilization efficiency, and infrastructure mechanization. We have public clouds and private clouds. These public clouds have been used by IT vendors for corporations to construct "private clouds" of their own. The concept or model called "pay as you go" is used to compute resources usage by end users. Public and private clouds use this model as well like the electricity system, telephone and internet systems [9]. However, so far clouds cannot be interoperating. Such federation or interoperating is called the Intercloud. Building the Intercloud needs more knowledge of their platform because of their different providers. It is important to prepare intercloud economy with a technically strong foundation and topology [16]. In general this paper deals with the security considerations of the intercloud.

IV. System Design And Implementation

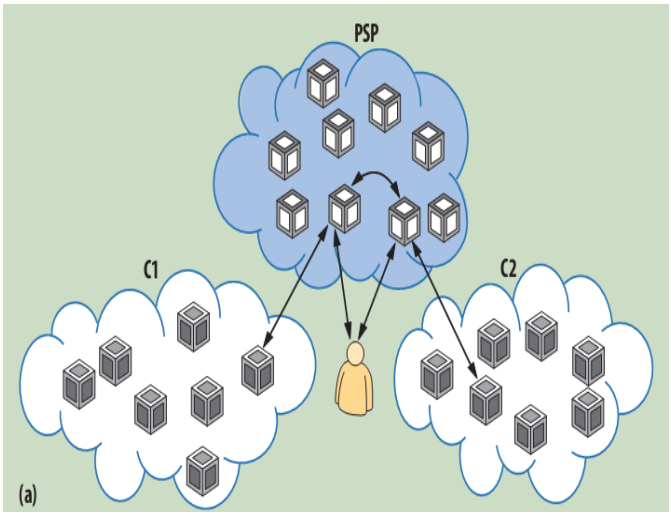

Fig 1 .A client employs two proxies to interact with CSPs C1 and C2

Implementation is an activity that brings the developed system into operational use and turning it over to the user. The changeover from the old to the new system can be arranged once the computer system is tested and approved. The most important phase in software life cycle is project implementation.

The initial process of project is to connect the user with server with the help of port number activation. According to the port number activation we have to connect the process with the cloud. Here, the data owner and also the data user can be connected with each other to put the IP address into the block. Main server can communicate with all users in the cloud and receive all information send by the users and also receiving the details. In that situation we provide the result of number of hosts, number of cloudlets and usage of particular virtual machines. These all information's are displayed in our process.

In download module the user has to know the file key to download the file. Again user has to login and give the file name to search. The download access is to enable the user and download the file. The downloaded file can be stored in any important drive in our system. The authorized user only can request the file and also access the file. If the owner enable the access rights to download the user has download the file easily. If the owner does not give the access rights to download the user can't download the file. In upload module the owner has to add the files.

To adding the file in the system the owner has to login his details first. The details are mail-id, password and his generated key. To upload the file the owner has to give the filename, keywords to identify the file, description about the file, permission access to read or write or both and file key. Then the owner has to choose the file and upload the file. The uploaded files are downloading by authorized users only. The unauthorized users do not download the files. The security can be maintained in this module.

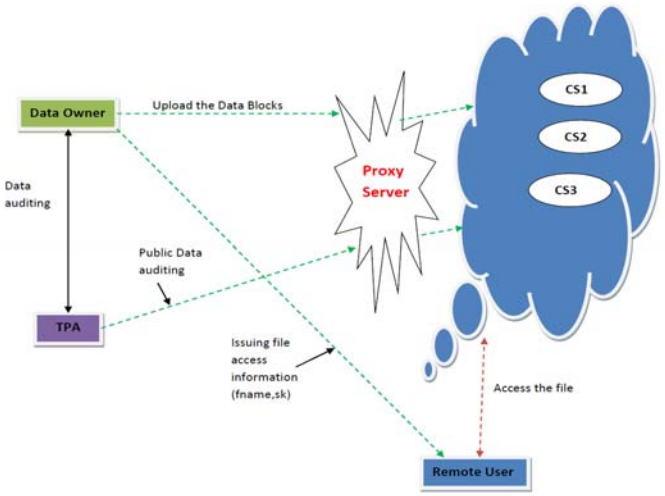

Fig 2. Architectural Design

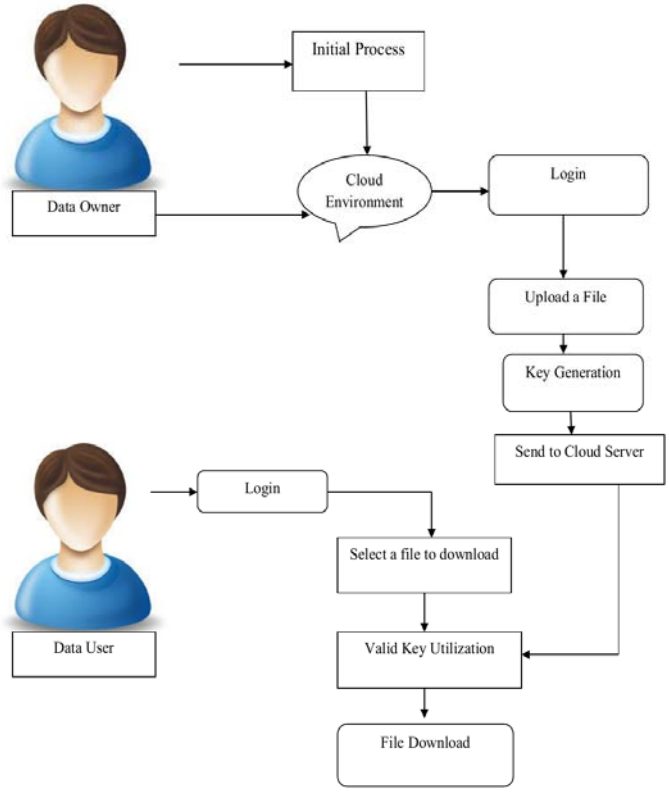

Fig 3. Data Flow DAigram

In dataflow daigram, initial process is to login into the cloud environment to upload the file. The file upload can be done by the data owner. In this process key generation is done for security purpose so once the data owner login into the cloud environment, next user gets the unique key. Now user has to verify his/her authentication with unique key, if it is corect then user can upload it otherwise it says invalid key.

Next step is for data user, here data user will download file from the cloud enviroment. In this step the aunthetication is done by key and data user will get the link to his/her mail id which file user needs to download.

V. RESULTS

Figure 4 shows the output for resource utilization for a perticuler user in multicloud computing environment. In this figure we can see the cpu, ram and bandwidth usage range of the perticuler user in graphical manner. In this graph, we have resources on y-axis and time on x-axis.

In figure 5 shows output for execution time of process and with help of clousimulator, we got some results based on the user usage of the system.In this figure we have time verses clouletId, which shows how much processes are been executed per seconds and depending on this we can decide whether user performing more tasks per second.

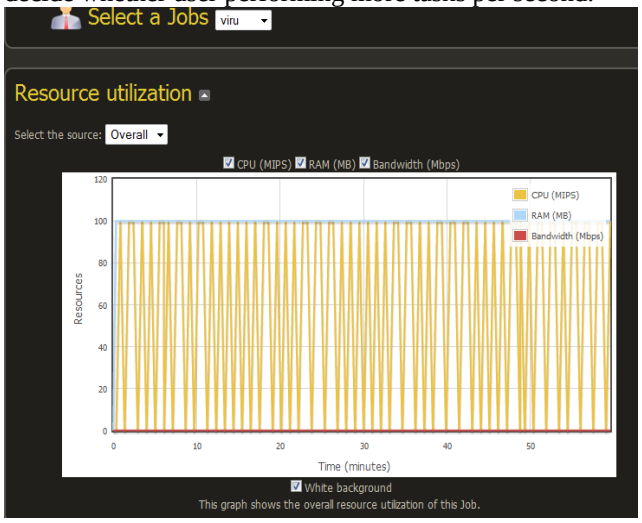

Fig 4. Resource Utilization

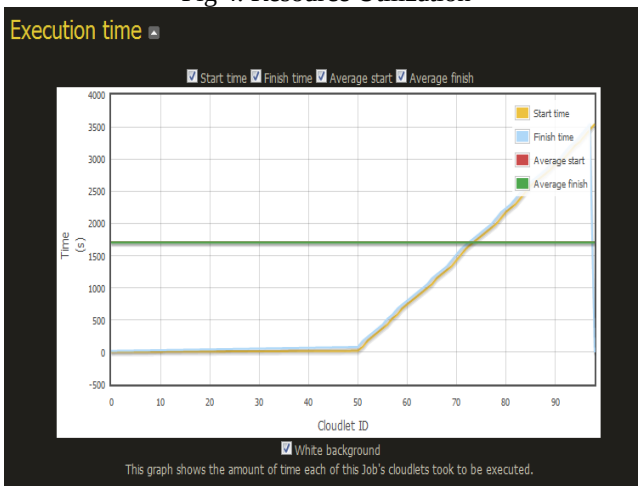

Fig 5. Execution Time

VI. CONCLUSION AND FUTURE WORK

It facilitates dynamic collaboration between clouds, in this proposed framework that uses proxies for collaboration between clouds. Here Proxies acts as a mediator between applications in multiple clouds that want to collaborate to share data. The proposed framework has the potential to overcome several restrictions in the current cloud computing model that can prevent dynamic collaboration among applications hosted by different cloud systems. Future research directions for the proposed framework include refining the proxy deployment scenarios and developmentof infrastructural and operational components of a multicloud system.

ACKNOWLEDGEMENT

The author thanks Dr. Annapurna P Patil for her constant guidance, encouragement and support. Her valuable guidance has provided the author with a deep insight into the topic.

REFERENCES

[1] Mukesh Singhal and Santosh Chandrasekhar, University of California, Merced Tingjian Ge, University of Massachusetts Lowell Ravi Sandhu and Ram Krishnan, University of Texas at San Antonio.

[2] B. Rochwerger et al., "*Reservoir—When One Cloud Is Not Enough*," Computer, Mar. 2011, pp. 44-51.

[3] S. Chandrasekhar et al., "*Efficient Proxy Signatures Based on Trapdoor Hash Functions,*" IET Information Security, Dec. 2010, pp. 322-332

[4] M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov./Dec 2011, pp. 74-79.

[5] Foued Jrad, Jie Tao and Achim Streit Steinbuch Centre for Computing, Karlsruhe Institute of Technology, Karlsruhe, Germany {foued.jrad, jie.tao, achim.streit}@kit.edu.

[6] David Bernstein, Deepak Vij Huawei Technologies, USA Huawei Technologies, USA.

[7] D. Bernstein and D. Vij, "*Intercloud Security Considerations,*" Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.

[8] Guilherme Sperb Machado, David Hausheer, Burkhard Stiller Communication Systems Group CSG, Department ofInformatics IFI, University of Zürich UZH Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

[9] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond and M. Morrow, Blueprint for the InterCloud Protocols and Formats for Cloud Computing Interoperability, In Proceedings of the Fourth International Conference on Internet and Web Applications and Services, 2009.

[10] B. Farroha and D. Farroha Cyber security components for pervasive Enterprise Security Management and the virtualization aspects, Systems Conference, 2010 4th Annual IEEE, 2010.

[11] Rochwerger B, Breitgand D, Levy E, Galis A, Nagin K, Llorente IM, Montero RS, Wolfsthal Y, Elmroth E,Cáceres JA, Ben-Yehuda M, Emmerich W, Galán F. The RESERVOIR model and architecture for open federated cloud computing.IBM Journal of Research and Development2009;53(4):1–11.

[12] Kelly K. The Technium: A Cloudbook for the Cloud. Available from: http://www.kk.org/thetechnium/archives/2007/11/a_cloudbook_for.php [last accessed 1 June 2012].

[13] Amazon. Summary of the Amazon EC2 and Amazon RDS Service Disruption. Available from: http://aws.amazon. com/message/65648/ [last accessed 1 June 2012].

[14] Google AppEngine, http://code.google.com/appengine/.

[15] Bernstein, D., Vij, D.: Using XMPP as a transport in Intercloud Protocols In Proceedings of CloudComp 2010, the 2nd International Conference on Cloud Computing (2010).

[16] Bernstein, D.: The Intercloud: Cloud Interoperability at Internet Scale, In Proceedings of the 2009 NPC, pp. xiii (Keynote 2), Sixth IFIP International Conference on Network and Parallel Computing (2009).

[17] "Xen hypervisor," http://xen.org/, May 2012.

[18] S. Crosby, R. Doyle, M. Gering, M. Gionfriddo, S. Grarup, S. Hand,M. Hapner, D. Hiltgen, and et.al, "Open Virtualization Format Specifi-cation," vol. DSP0243 1.1.0, Jan 2010, http://dmtf.org/standards/ovf.

[19] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Kakata,J. Pruyne, J. Rofrano, S. Tuecke, and M. Xu, "Web Services Agreement Specification (WS-Agreement)," vol. GFD.192, October 2011, https://forge.ogf.org/sf/projects/graap-wg.

[20] B. Allcock, J. Bester, J. Bresnahan, A. L. Chervenak, I. Foster, C. Kesselman, S. Meder, V. Nefedova, D. Quesnal, S. Tuecke. "Data Management and Transfer in High Performance Computational Grid Environments", Parallel Computing Journal, Vol. 28 (5), May 2002, pp. 749-771.

[21] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3, 2008.

[22] J.Brodkin. "Gartner: Seven cloud-computing security risks",http://www.networkworld.com/news/2008/070208cloud.html, 2008.