REVIEW ON SECURITY BASED ON MULTIPLE CLOUD COMPUTING

[1]MRUNALI KHEDIKAR, [2]SULABHA PATIL, [3]RAJIV DHARASKAR

[1]Mtech student, [2]Assistence professor, [3]Assistence professor
[1,2,3]Computer Science and Engineer,Department of M. Tech CSE
Tulsiramji Gayakwad-Patil College of Engineering and Technology Nagpur,India
E-mail: [1]mrunali7khedikar@gmail

Abstract- Cloud service provider basically provides Software, Platform and infrastructure as service to the user on pay-per-use basis. When the user gains a service from a cloud gets vendor lock-in and has to avail all services from a single cloud provider, while data confidentiality solutions for paradigm are still immature. As organizations are now adopting the cloud environment the cloud service providers are now moving towards a new concept i.e. multiple cloud where a user can utilize services from multiple cloud service provider. We proposed secured proxy-based multi-cloud computing framework allows dynamic, on the- fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues. We integrates cloud with data confidentiality and the possibility of executing concurrent operations on encrypted data. These multi-clouds are organized by an agreement between different service providers to provide a functionalities to the client. Multiple cloud where a user can utilize services from multiple cloud service provider.

Keywords- Cloud Computing, Cloud Service Provider (CSP), File Upload, File Download.

I. INTRODUCTION

The cloud computing model represents a new paradigm shift in internet-based services that delivers highly scalable Distributed computing platforms in which computational resources are offered 'as a service'. Cloud computing characteristics include a network-based access channel; resource pooling; multi-tenancy; automatic and elastic provisioning and release of computing capabilities; Clouds can dynamically provision these virtual resources to hosted applications or to clients that use them to develop their own applications or to store data. Rapid provisioning and dynamic reconfiguration of resources help cope with variable demand and ensure optimum resource utilization. We can extract the maximum efficiency from the cloud computing. And the users can access the cloud environments. There are a large number of cloud service providers as of now. Some of them are Microsoft, Amazon, IBM, Oracle, and PeopleSoft and so on. These companies make the cloud business & provide a variety of services. The service models of cloud include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). The users can use these services according to need. The services provided by the cloud are cheaper, therefore the organizations across the world can grow faster. More users can be attracted towards cloud by providing high security. Multiple cloud-based services, like cloud mash-ups, opens up opportunities for CSPs to offer more-sophisticated services that will benefit the next generation of clients.

Cloud service providers are supposed to provide high security to cloud services in order to attract more users towards cloud. There is an important observation that a single cloud has certain concerns. For instance it may cause failure, insider theft, service availability problems and so on. To overcome this problem there exists research towards moving to multi-cloud environments. In multi-cloud environments, there will be more chances to have 24/7 service availability, security and reduced risk to the stored data. A common concern in a multi-cloud environment is that the integrity of data, shared across multiple users, may be compromised [3]. Moreover, choosing an ideal vendor to provide secure and guaranteed collaboration service is also non-trivial [4]. Nevertheless, mash up in multi-cloud has become not only valuable but also essential as it allows the organizations to easily connect with artners, customers, and employees from remote locations with less communication latency.

II. RELATED WORK

This is a review paper based on the research work done by the researcher in the field of a new environment in cloud computing i.e. the collaboration of multi-cloud. This will give an overview of the techniques which will be helpful for shifting from the single cloud architecture to multi-cloud architecture, a security model and cost effectiveness of multi-cloud compared to a cloud. This section reviews literature that has been available on cloud computing security issues and other related topics. There were many researches that focused on cloud computing security issues. For instance in [1] multi-shares was proposed that makes use of secret sharing algorithm Single cloud environment issued in [2] to solve service availability problem. The main issue in implementing multi-cloud is its working in a distributed environment as the services are to be collaborated with different cloud service providers to make it

possible a framework is laid in the research work of "Collaboration Framework for Multi-cloud Systems" [5] which specify the use of proxies at different level of collaboration. These proxies can be implemented by the cloud service provider or can be set by the institutions\organization so as to gain service from collaborated service providers. These proxies can also be used to have a secure communication between the client and the service provider. To protect data at rest and data in transit, proxies must provide a trusted computing platform that prevents malicious software from taking control and compromising sensitive client and cloud application data [5]. This also deals with the security aspect of the cloud computing. There were many researches that focused on cloud computing security issues. For instance in [6] multi-shares was proposed that makes use of secret sharing algorithm. Cryptographic methods were explored in [7] for protecting cloud services. Many security risks are addressed including data integrity, service availability and data intrusion. This is achieved using multi-clouds. cloud mash up is achieved by prior business agreements among the cloud providers and this limits the security to the individual cloud. Single cloud environment issued in [8] to solve service availability problem. Cloud security issues were discussed in [9] and the cryptography is used as security solution in [10] single cloud contexts. "Depot" is the security mechanism proposed in [11] in single cloud context. Another security mechanism by name "Venus" is used in [12] for data integrity in the single cloud context. In [13] service availability is focused while in [14] a survey is made on security in the single cloud environment. Another security mechanism by name "HAIL" was introduced in [15] in order to improve service availability. This work is done in multi-cloud environments. A survey was made in [16] in multi-cloud environment with respect to data integrity.Moreover our proposed cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. This provides security to the data by providing access control to the clients.

III. PROPOSED ALGORITHM

Independent systems dynamically come together to share information for a period of time. No global policy is maintained as interoperation requests are "on-demand" to facilitate dynamic data sharing. In a cloud environment, both tight and loose coupling may take place depending on the nature of collaboration. For example, if different departments of an organization collaborate using cloud services, it is an instance of tightly-coupled collaboration. However, if autonomous domains mash-up "ondemand" for a limited period of time, it is an example of loosely-coupled collaboration. For both collaborations, if multiple collaboration requests are generated within the same period of time or perticuler session.

A. Some specific security issues associated with collaboration among heterogeneous clouds include:

- establishing trust among different cloud providers to encourage collaboration;
- addressing policy heterogeneity among multipleclouds so that composite services will include effective monitoring of policy anomalies to minimize security breaches; and
- Maintaining privacy of data and identity during collaboration.

B. Design Considerations:

- A user can utilize services from multiple cloud service provider.
- These multi-clouds are organized by agreement between different service providers to provide a Low cost functionalities to the client.
- Thus solves the problem of vendor lock in
- Proxy service provider provides secured communication between the cloud.

C. Description of the Proposed Algorithm:

Aim of the proposed algorithm is to mash up in multiple cloud to supports universal and dynamic collaboration in a multicloud system.

Clouds consist of multiple network-connected resource such as server farms, data warehouses, and so on that host geographically distributed virtual machines and storage components that ensure scalability, reliability, and high availability.

A multi-cloud system that employs proxies for collaboration consists of three architectural components: multiple cloud computing systems, proxy service provider, and clients (or service users). Such systems can use several possible strategies for placing proxies in a proxy network.

A client must register himself before his first login for obtaining access to the content in the cloud. The details at login are verified with the one stored in server before granting access. The rescind users will not get access as their profile is updated in the server to make him remain block forever.

The feature that a client can get the contents stored in the cloud only after the verification of the authentication of the client through the registered email. The collaboration between the clouds can only done by Proxy service provider, user or admin can't connect directly to other clouds.

IV. CONCLUSION AND FUTURE WORK

In present SaaS clouds, online mash up is one of the popular offerings. However, ensuring secure and fair mas-up among participating domains is a challenging task. owing of cloud-based collaboration, interoperation requests from a remote user are sent in form of a set of permissions. we propose a distributed secure collaboration framework for cloud mash-up service. Cloud computing technology has grown to the extent where users can store their confidential data in cloud storage. Outsourcing such data to cloud has plethora of advantages. But the cloud users have security concerns as the cloud service providers usually do not take care of complete end to end security of cloud data. To address the security concerns of cloud users, in this paper, we implemented a multi-cloud environment where users can store data in multiple clouds. The advantages of this kind of environment include high service availability, low security risks and the insider theft is eliminated to a greater extent.

REFERENCES.

[1] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-service", 44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.

[2] A.J. Feldman, W.P. Zeller, M.J. Freedman andE.W. Felten, "SPORC: Group collaboration usinguntrusted cloud resources", OSDI, October2010, pp. 1-14.

[3] H. Li, B. Wang, and B. Li, “Oruta: Privacy-preserving public auditingfor shared data in the cloud,” IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43–56, 2014.

[4] N. Ghosh, S. Ghosh, and S. Das, “Selcsp: A framework to facilitate selection of cloud service providers,” IEEE Transactions on Cloud Computing, 2014, doi: 10.1109/TCC.2014.2328578.

[5] Ana Juan Ferrer, Francisco Hernándezb, Johan Tordsson , Erik Elmroth, Ahmed Ali-Eldin, Csilla Zsigri, Raül Sirvent, Jordi Guitart, Rosa M. Badia, Karim Djemamee, Wolfgang Ziegler, Theo Dimitrakos, Srijith K. Nair, George Kousiouris, Kleopatra Konstanteli, Theodora Varvarigou, Benoit Hudzia, Alexander ipp, Stefan Wesnerj, Marcelo Corrales, Nikolaus Forgó, Tabassum Sharif, Craig Sheridan, “OPTIMIS: A holistic approach to cloud service provisioning”, Future Generation Computer Systems ELSEVIER pp. 66–77, 2012.

[6] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.7

[7] Bessani, M. Correia, B. Quaresma, F.André andP. Sousa,"DepSky: dependable and secure storagein a cloud-of-clouds", EuroSys'11: Proc.6thConf. OnComputer systems, 2011, pp. 31-46.

[8] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration usinguntrusted cloud resources", OSDI, October2010, pp. 1-14.

[9] E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", EEESecurity & Privacy, 8(6),2010, pp. 17-23.

[10] S. Kamara and K. Lauter, "Cryptographic cloudstorage", FC'10: Proc. 14thIntl.Conf. on inancialcryptograpy and data security,2010, pp. 136-149.

[11] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi,M. Dahlin and M. Walfish, "Depot: Cloud storagewith minimal trust", OSDI'10: Proc. of the 9thUSENIX Conf. on Operating systems design andimplementation, 2010, pp. 1-16.

[12] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y.Michalevsky and D. Shaket, "Venus: Verificationfor untrusted cloud storage", CCSW'10: Proc.ACM workshop on Cloud computing securityworkshop, 2010, pp. 19-30.

[13] S. Subashini and V. Kavitha, "A survey on securityissues in service delivery models of cloudcomputing", Journal of Network and ComputerApplications, 34(1), 2011, pp 1-11.

[14] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Securityand Privacy Challenges in Cloud ComputingEnvironments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[15] K.D. Bowers, A. Juels and A. Oprea, "HAIL: Ahighavailability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. onComputer and communications security, 2009, pp.187-198.

[16] C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[17] Analysis of Various Digital Forensic Techniques for Cloud Computing D. Shirkhedkar, S Patil International Journal of Advanced Research in Computer Science 5 (4)

[18] Analysis of online messages for identity tracing in cybercrime investigation SM Nirkhi, RV Dharaskar, VM Thakre Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012

[19] Design of digital forensic technique for cloud computing D Shirkhedkar, S Patil International Journal 2 (6)

★★★