IJCSN International Journal of Computer Science and Network, Volume 5, Issue 3, June 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Mash-Up in Multiple Cloud Computing With Security

[1] Mrunali Khedikar, [2] Sulbha Patil, [3] Rajiv Dharaskar

[1] Computer Science and engineering, RTMNU, TGPCET
Nagpur, Maharashtra, India

[2, 3] Computer Science and engineering, RTMNU, TGPCET
Nagpur, Maharashtra, India

Abstract - Cloud computing obtaining huge attention due to its characteristics and services provided by it as Software, Platform and infrastructure as service. Nowadays cloud computing became as a popular paradigm that offers computing resources as scalable and on-demand, on fly collaboration, resource sharing services over the Internet on the basis of pay per use. With single cloud user gets vendor lock-in and use all services from single cloud in which data confidentiality is still immature. The user can gain services from single cloud provider there is risk of data theft, failure and service availability problems. This problem can be addressed by moving from single to multiple cloud thus having more options that can reduce risk and improve availability of service and increase complexity of data availability. Mash-up will be driven by the growing need to offer diverse services without having to spend heavily on infrastructure. In this paper we propose novel architecture of multiple cloud computing mash-up, executing concurrent operations on encrypted data for security purpose and end to end data protection by generating secrete key. We have developed a proof of concept of our framework using java and deployed it on a RH cloud.

Keywords - *Mash-Up, Security, Multiple Cloud, File Upload, File Download.*

1. Introduction

The service models of cloud include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS).

- Cloud Software as Service: This is a capability in which the consumer can use the provider's applications running on the cloud.
- Cloud Platform as Service: In this type of service, the consumer can deploy, the consumer created or acquired applications created by using programming languages or tools provided by provider, on the cloud infrastructure.
- Cloud Infrastructure as Service: This is a capability provided to the consumer by which, it can provision processing, storage, networks and other fundamental computing resources where the consumers can deploy and run the software

The users can use these services according to their 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. The term cloud computing can be defined as "a system that is concerned with the integration, virtualization, standardization, and management of services and resources". The profits of cloud computing incorporate minimized capital use, usage and proficiency change, high registering force, area, gadget freedom also at last high adaptability, improve security, utilization and efficiency improvement, high computing power, location and device independence and finally very high scalability [1].

Our proposed framework for generic cloud mash-up allows clients and cloud mash-up 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 multi-cloud system. Thus we can avoid the vendor lock-in syndrome. A cloud is an edge node hosted software instance that a client or a CSP can delegate to carry out operations on its behalf. Depending on the context, the system can regard a network of mash-up as a collection of multiple cloud connected for particular period of time. The basic idea it to enable that act on behalf of a subscribing client or a

cloud to provide a diverse set of functionalities. Our project 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. In a multi-provider hosting scenario, the Service Provider is responsible for the multi-cloud provisioning of the services. Nowadays, cloud require 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. There is no need of pre-established collaboration agreements or standardized interfaces. Realizing multi-cloud mash-up full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services spread across multiple clouds.

In this paper we provide mash-up between clouds, consider a case in which a multiple vendor wishes to simultaneously use a collection of services that multiple clouds offer.

Thus, assuring the private and consistent management of information relevant to becomes more complex in multi-cloud system. 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, end to end security will be provided. The data is retrieved only after security verifications. The internal theft is not possible because of data stored in multiple cloud and the data availability is enhanced besides reducing the risk of security. Encryption will be provided to whatever data we store in the multiple cloud and secrete key is generated for security. By using multiple cloud mash-up, vendor lock-in can be abolished with an agreement between the various cloud service providers that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement. The main objective of our project is “To provide high availability, eliminate vendor lock-in issue, establishing trust and secure delegation.”

2. Literature Review

This section review literature on the basis of work done in the area of a new environment in cloud computing i.e. the mash up of multiple cloud. This will give an overview of the techniques which will be helpful for moving from the single cloud to multi-cloud architecture, a security model of multi-cloud compared to a cloud. Main aim that is focus on mash-up in multiple cloud and end to end data protection. The principle issue in actualizing multi-cloud is its working in a distributed environment as the services are to be teamed up with distinctive cloud service providers to make it conceivable a schema is laid in the exploration work of "Collaboration Framework for Multi-cloud Systems" [2] which detail the use of proxy at different levels of collaboration. 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.

The principle issue in actualizing multi-cloud is its working in a distributed environment as the services are to be teamed up with distinctive cloud service providers to make it conceivable a schema is laid in the exploration work of "Collaboration Framework for Multi-cloud Systems" [2] which detail the use of proxy at different levels of collaboration. These proxies could be actualized by the cloud service provider or can be set by the institutions\organization in order to increase administration from collaborated service providers. These substitutes can likewise be used to have a secure communication between the customer and the service provider. To protect stored data and data in transit, proxies must provide a trusted computing platform that keeps noxious programs from taking control and compromising sensitive customer and cloud requisition information [2]. No experiments have been conducted [2] .In which main objective “Ensure security for dynamic collaborations and resource sharing among multiple clouds which do not have any pre-established collaboration agreement or standardized interfaces”

[3]For cloud-based collaboration, the participating domains have to strictly use vendor provided APIs to model access policies. Presently, cloud vendors use token-based authentication scheme, eliminating the need for sensitive credential information. Such token uses scopes of access modes (read, write, execute, etc.) to determine the privilege level on the requested object. Generally, a resource provider issues access tokens to the requesting applications, thus specifying the allowed level of access. At the time of request, the application attaches this access token with the hashed code of object. If the request and the token are found to be valid, access is granted, until the token is timed out. As such authorization is not based on the properties of requesting entity, trust is not generated before granting access to any resource. Therefore, the use of trust management systems is not realistic in cloud scenario. A major challenge with this interface role is deciding its permission set.

Another security mechanism by name “HAIL” was introduced in [4] in order to improve service availability.

This work is done in multi-cloud environment. A survey was made in [5] in multi-cloud environment with respect to data integrity. Authorizing collaborations among services hosted in different clouds [6]. Main objective is the authors proposed a model checking technique based on RBAC reasoning. It acts as a management service/tool for verification of access policies from multiple domains. Based on these policies, domains interoperate in a cloud environment. The verification process combines all the policies from different domains and carries out compliance checking. This approach deals with detection of access conflict, but does not handle their removal. The result is Simulation of collaborating domains and roles done and experiment results showing the performance of the verification process (both normal and optimized) are given. However, performance evaluations with respect to domains or roles is not done.

In [8] service availability is focused while in [7] a survey is made on security in the single cloud environment. In this focus is on enable users to manage access policies for controlling to access to heterogeneous resources deployed over multiple cloud environments, the authors propose a framework for policy management service provider (PMSP) that enables users to define, edit and manage accesses. Important steps of operation are: (i) registration to PMSP, (ii) resource discovery, (iii) access policy specification, and (iv) Translating and exporting policies to cloud providers. In this No experiment results given.

Cryptographic methods were explored in [9] for protecting cloud services. Many security risks are addressed including data integrity, service availability and data intrusion. This is achieved using multi-clouds. A survey was made as explored in [10] to know the things going on in the industry with respect to cloud computing. The survey focused on security issues and moving towards from single to multi-cloud. RAID and RACS are the techniques used in [11] for securing multi-clouds. Distributed protocols which are client centric are explored in [12]. Such protocols are client centric and provide data integrity in multi-cloud environments. Single cloud environment issued in [13] to solve service availability problem. Cloud security issues were discussed in [14] and the cryptography is used as security solution in [15] single cloud contexts. "Depot" is the security mechanism proposed in [16] in single cloud context. Another security mechanism by name "Venus" is used in [17] for data integrity in the single cloud context.

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 multi-cloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

3. Our APPROACH

Independent systems dynamically come together to share information for a period of time. We are using Loosely-coupled collaboration in this collaboration, 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 loose coupling may take place depending on the nature of collaboration. "If autonomous domains collaborate "on-demand" for a limited period of time" it is example of loosely couple collaboration. For security we provide the key generation algorithm in which admin can send secrete key to vendor on register email id without this he is not able to access the file. It is the process which provides security to the whole data which present in the cloud environment. Clouds provide multiple services to the user such as download, and a cloud provides limited services to an individual user. The *MD5 Message-Digest Algorithm* is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value.

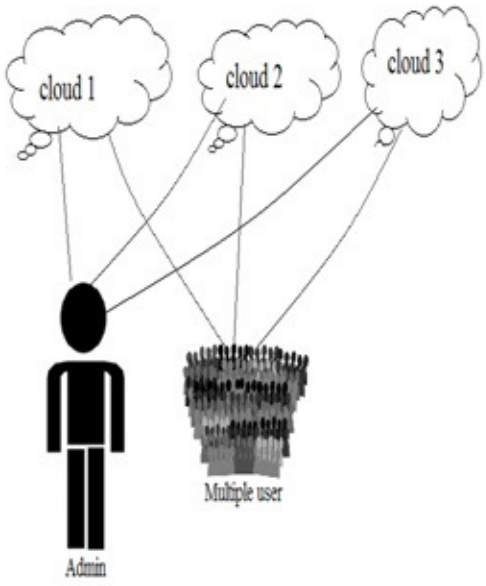

Fig: Multiple cloud architecture

- 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

4. Methodology and Implementation

The project is implemented in java Netbeans is the IDE used for the project development. In our project any type of file will be uploaded and downloaded from anywhere in the world. The framework is provided by cloud hosting site i.e. RH.com. We are creating two cloud i.e. cloud1 and cloud2.

4.1. GUI

This framework will be provided by the cloud hosting site i.e. Rh.com i.e. cloud 1 and cloud 2

Admin login
Vendor loin

Fig: graphical user interface (cloud 2)

4.2. Admin as Proxy

Admin will create the environment for the cloud application to run on any cloud service provider as in here, RH.com. Steps are as follow.

- Admin will login into his account and manage his own data i.e. upload from anywhere he wants.
- There is an option for file upload
- Admin can manages all file at time from any cloud i.e. if data is stored from any cloud but he handle it from another cloud or cloud itself. It is nothing but Admin will able to see data which is previously uploaded.
- Uploaded data is store in the encrypted form.
- He is also able to download file if he need in future.
- Admin is also able to delete the file if there is no need of file in cloud.
- Data is stored in multiple cloud due to which complexity increases.
- Add vendor option from which admin can added vendor in which the email-id is unique. And also see vendor list.
- From which admin can grant the access of particular file to vendor which send by vendor request for particular file access
- RH.com is the CSP in this project that works as administrator
- This module has been implemented successfully and working

Fig: Admin as proxy (cloud 2)

4.3. Vendor/User

User is the one who wants to avail the service from the cloud service provider. Here in this project user avails the storage service from the cloud. User First of all registers himself through admin & gets username & password to avail such service. When user needs to download any file on the cloud he has to login first.

After login there he comes across two options Download file. There will be a dropdown list of all the files store He send request for particular file After grant request, user can put the secret key that is send on registered email id for file access. User can use both these services from any location he just needs an internet connection on the device he is using.

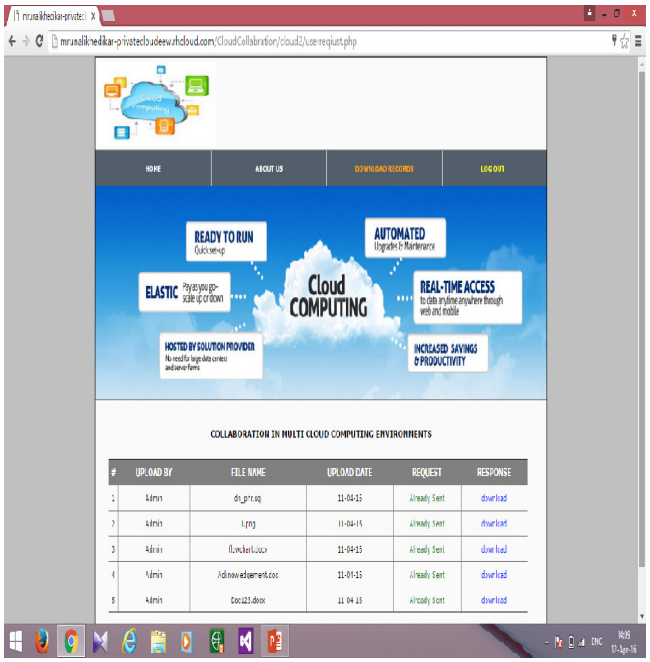

Fig: vendor form (cloud1)

4.4. Mash-up of multiple Cloud

File which is stored in the multiple cloud i.e. cloud1 and cloud2 is collected and download after finishing the steps of the vendor. Data is collected from multiple cloud for particular duration.

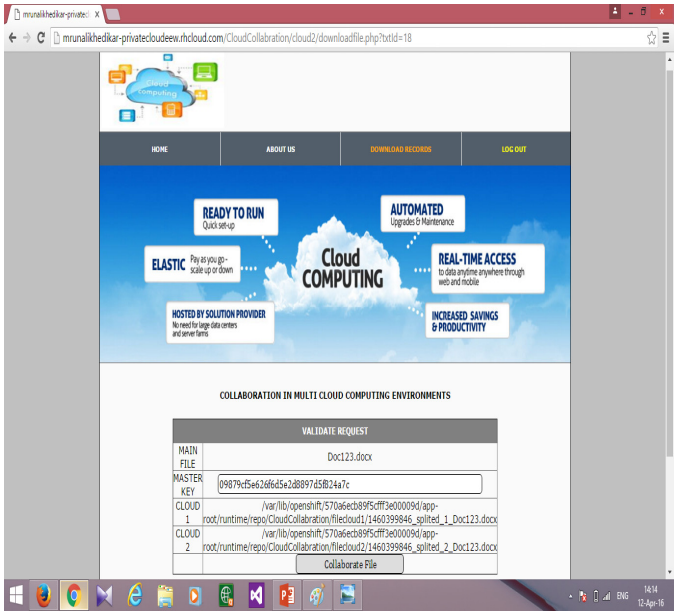

Fig: mash up of multiple cloud

5. Conclusion and Future Scope

Cloud computing technology has grown to the extent where users can store their confidential data in multiple cloud storage. The multiple cloud environment can finished the vendor lock-in of the consumer which is attained in the single cloud. The profit of this kind of Framework include high service availability, low security risks and the insider theft is eliminated to a greater extent. In this paper, we proposed a secure multiple cloud computing mash-up which facilitates collaboration between clouds and gives the admin has opportunity to download the files from different cloud and allow user to download the file which is present. Future scope of this framework is backup for maintaining the data.

References

[1] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. Saleem Durai, "Secured Multi-Cloud Virtual Infrastructure with Improved Performance", cybernetics and information technologies XII, (2), pp. 11-22, 2012

[2] Mukesh Singhal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-Joon Ahn, and Elisa Bertino "Collaboration in Multicloud Computing Environments: Framework and Security Issues", Published by the IEEE Computer Society IEEE, 2013.

[3] Ayad Barsoum and Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE transactions on parallel and distributed systems

[4] 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.

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

[6] A. Gouglidis, I. Mavridis, and V. C. Hu, "Security policy verification for multi-domains in cloud systems," International Journal of Information Security, vol. 13, no. 2, pp. 97–111, 2014.

[7] 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.

[8] 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.

[9] A. 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.

[10] F. Rocha and M. Correia, "Lucy in the Sky withoutDiamonds: Stealing Confidential Data in theCloud", Proc. 1stIntl. Workshop of Dependabilityof Clouds, Data Centers and Virtual ComputingEnvironments, 2011, pp. 1-6.

[11] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.

[12] C. Cachin, R. Haas and M. Vukolic, "Dependablestorage in the Intercloud", Research Report RZ,3783, 2010.

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

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

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

[16] 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.

[17] 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.