A Novel Approach for Framework and Security Issues Cooperation in Multicloud Computing Environment

kediga pallavi[1], Narsimha Banothu[2], Janapati Venkata Krishna[3]

[1]*pursuing M.Tech (CSE), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

[23]*working as Associate Professor (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

***Abstract*— A proposed proxy-based multi-cloud computing structure allows dynamic, on the fly collaborations and resource split among cloud-based services, addressing trust, policy, and privacy concern without pre-established collaboration agreements or standardized computing. The recent surge in cloud computing arises from its capability to provide software, infrastructure, and platform assistance without requiring large investments or outlay to manage and operate them. Clouds typically require service providers, infrastructure/resource providers, and service users (or clients). They incorporate applications delivered as services, as well as the hardware and software systems presuming these services. Cloud computing aspects incorporate a pervasive (network-based) access channel; resource pooling; multi-tenancy; automatic and elastic provisioning and release of computing capabilities; and metering of resource usage (typically on a pay-per-use basis). Computing of resources such as processors, network, memory, and storage establish scalability and high availability of computing capabilities. Clouds can dynamically providing these virtual resources to hosted applications or to clients that use them to develop their own applications or to store data. Rapid providing and dynamic reconfiguration of resources help cope with variable demand and ensure optimum resource utilization.**

***Keywords*— Multi Cloud, Cloud service Provider, Proxy service Provider.**

I. INTRODUCTION

Cloud is defined as typically complicated service providers' infrastructure/resource providers, and service users (or clients). They incorporate applications dispatch as services, as well as the hardware and software systems presuming these services.

Cloud computing features incorporate a ubiquitous (network-based) access channel; resource pooling; multi-tenancy; automatic and elastic provisioning and release of computing capabilities; and metering of resource usage (typically on a pay-per-use basis). In Computing of resources such as processors, network, memory, and storage establish scalability and high availability of computing capabilities. Clouds can dynamically provide these virtual resources to hosted applications or to clients that use them to develop their own applications or to store data. Instant provisioning and dynamic reconfiguration of resources help cope with variable demand and ensure prime resource utilization.

As more organizations adopt cloud computing, cloud service providers (CSPs) are developing new technologies to enhance the cloud's capabilities. Cloud fusion is a recent trend; fusion combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services.

II. RELATED WORK

Many existing cloud data services provide indistinguishable access control models, in which individual and organizational solitude, a key requirement for digital affinity management, is unprotected. Also with cloud computing initiatives, the scope of insider threats, a major source of data theft and privacy breaches, is no longer limited to the organizational perimeter. Multicloud environments aggravate these issues because proxies can access data (which the environment might dynamically move or partition across different clouds) on behalf of clients. Knowing sensitive information in identity attributes to proxies that grant them authorization to access the data on behalf of clients is not an attractive solution. Thus, reassure the private and consistent management of information relevant to attribute based access control (ABAC) becomes more complex in multicloud systems.

III. COLLABORATION FRAMEWORK FOR MULTICLOUD SYSTEMS

Our proposed framework for generic cloud collaboration allows clients and cloud applications to together use services from and route data among multiple clouds. This framework supports common and dynamic collaboration in a multi cloud system. It lets clients together use services from multiple clouds without prior business agreements among cloud providers, and without appropriate common standards and specifications. As more organizations acquire cloud computing, cloud service providers (CSPs) are developing new technologies to intensify the cloud's capabilities. Cloud mash ups are a recent trend; mash ups combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services. This service constitution lets CSPs offer new practicality to clients at lower development costs.

In the current environment, a client that wishes to together use services from multiple clouds must individually interact with each cloud service, gather inter-mediate results, process the collective data and generate final results.

IV METHODOLOGY

Clouds consist of multiple network-connected resource clusters such as server farms and data warehouses that host geographically distributed virtual machines and storage components that confirm scalability, reliability, and high availability. Multicloud system that employs proxies for collaboration consists of three architectural components: multiple cloud computing systems, networks of proxies, and clients (or service users).

In cloud computing, subscribers have to pay the service providers for the storage service. This service not only provides flexibility and scalability for the data storage, it also provide customers with the feasibility of paying only for the amount of data they need to store for a particular period of time, without any concerns for effective storage mechanisms and maintainability issues with large amounts of data storage.

The cost effectiveness of deployment of cloud depends upon the deployment of virtual infrastructure it also affects whether it is static or dynamic deployment. Researchers interest only on static

deployment where the user of service providers' condition does not change but in some cases the deployment has to be changed according to the time factor so as to be cost effective. Cloud computing can be categorized as a new paradigm for the dynamic provisioning of computing services supported by state-of-the-art data centers that usually employ Virtual Machine (VM) technologies for consolidation and environment isolation purposes.

PROXY BASED FRAMEWORK

A proposed proxy based multi cloud computing framework enable dynamic, on the fly collaborations and resource sharing among cloud depended services, addressing trust, policy, and privacy issues without pre established collaboration agreements or assimilate interfaces. It include the use of proxy in multi cloud environment in various forms these are

Cloud-Hosted Proxy:

In this framework the cloud service provider host proxies within its infrastructure administer and manage the proxies and will handle the service request from the client who wants to access these proxies.

Proxy as a Service:

Here the proxy is been deployed as an individual cloud. Multiple cloud service providers with collaboration can manage this proxy or a third party proxy service provider can manage it for the cloud service providers.

Peer-To-Peer Proxy:

Proxy can also be communicated on peer-to-peer network which is managed by the proxy service provider or cloud service provider those who have an agreement of collaboration.

On-Premise Proxy:

The client himself can host proxies within infrastructural domain and manage it in administrative domain. The person who wishes to use proxies will have to deploy it on premise proxies and the service providers that wish to collaborate with other service provider will have to implement it within the service requesting client domain.

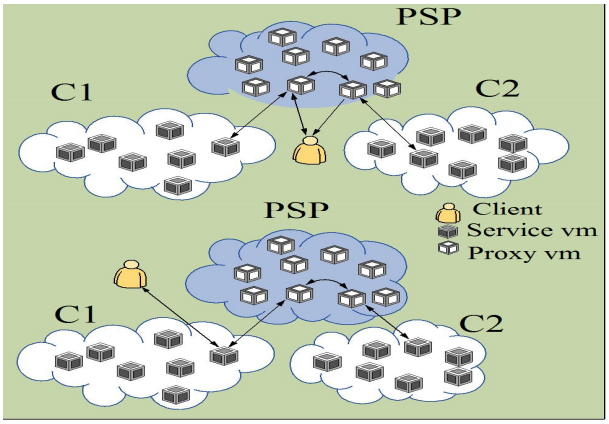

Fig 1: **Proxy as a service. Cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients.**

SECURITY ISSUES

Sharing applications that process critical information with different tenants without sufficient proven security separation, security SLAs or tenant control, results in loss-of-control and lack of trust problem. Using proxies moves the trust perimeter one step further: clients and CSPs now must establish trust relationships with proxies, which incorporates accepting a proxy's security, reliability, availability, and business continuity guarantees. A sensible collaboration must be set between the client and Cloud service provider which will help in management and administering proper communication. In this architecture different types of proxies network is been explained some are CSP's side and some are established on client side this states the control over the assets while processing proxies and similarly using proxies that are within the domain of cloud service provider exercise its control over proxies management.. Proxy network is a potential platform for developing proxy based security architecture. Data confidentiality in transmission in proxy based network can be achieved using Transport Layer Security Protocol. Some technologies that can be used to provide security are warrant-based proxy signature for delegation signing rights to provide authentication to the proxies and simple public - key infrastructure can provide secure access and authentication.

MULTI-CLOUD PaaS INFRASTRUCTURE

This infrastructure offers some solutions to the problems such as portability and interoperability for management of both SaaS and PaaS. The disparate layers of a cloud environment (Saas, IaaS, and PaaS) provide dedicated services. However their granularity and complexity vary, we convinced that a principled definition of these services is needed to promote the interoperability and federation between heterogeneous cloud environments.

This integrated infrastructure is based on following three models:

Open Service Model

The disparate layers of a cloud environment (Saas, IaaS, and PaaS) provide dedicated services. However their granularity and complexity vary, we believe that a principled definition of these services is needed to promote the interoperability and federation between heterogeneous cloud environments. A Service Component Architecture is designed for running service oriented distributed applications. Its supports interaction between different protocols for this it has a notion of binding. Hence SCA is used for both the definition of services in federated PaaS and services of SaaS.

Multi - PaaS Infrastructure

This multi-PaaS architecture depends on configurable substance which can be accomplished in concrete cloud environment. A Software product line can be defined as a set of software intensive system that share a common, managed set of features and that are developed from a common set of core assets in a prescribed way. The basic idea of defining the software product line is to capture the points of variability between the cloud environments and implement as a component of Secure Component Architecture.

Infrastructure Services

A generic architecture has been laid down by the definition of Service component architecture and configurable substance in this environment a cloud that hosts SaaS is considered as a node and configurable substance as an instance for particular cloud. The service list first allocates the resources on all nodes and then deploys the configurable substance and applications on each node the second step involves the deployment of instances of configurable substance and applications on particular node as both the PaaS and SaaS are based on service component architecture they can be deployed either on the substance level or on the application level.

IDENTITY ATTRIBUTES AND DATA PRIVACY

In shared computing environments like clouds, protecting the privacy of client assets is critical. The privacy issues pertaining to both data and identity.

Identity attributes privacy

Data as a service (DaaS), such as Amazon S3 and Microsoft Azure, is an emerging cloud service in which organizations can seamlessly store data in the cloud and retrieve it based on access control policies that cover legal requirements and organizational policies. An expressive access control model, such as XACML, can specify access control policies on protected objects in terms of a subject's properties, called *identity attributes*. These can incorporate a subject's email address, organizational role, age, and location of access. Such an *attribute-based access control* (ABAC) model provides fine-grained data access and expresses policies closer to organizational policies.

A crucial issue in this context is that identity attributes required by subjects to access protected objects often encode sensitive information. Many existing cloud data services provide similar access control models, in which individual and organizational privacy, a key requirement for digital identity management, is unprotected.

In multicloud environments, where proxies use attribute based access control (ABAC) to retrieve client data from the clouds, clients need to hide their identity attributes from both proxies and Cloud Service Providers to preserve the privacy of sensitive client information. However, clients must still give proxies the information that grants them access to requested data. This requirement calls for the use of identity attribute and data encoding techniques that, used together, permit oblivious data transfer between Cloud Service Providers, proxies, and clients while presuming privacy-preserving ABAC.

The techniques for encoding client identity attributes must permit clients to transfer the encoded attributes to proxies; the proxies, in turn, must convince Cloud Service Providers of the ownership and validity of the encoding, without having the client reveal its identity attributes to either entity. Data and identity attribute encoding techniques must ensure that decoding the data is possible when the identity attributes match the attribute based access control (ABAC) policies, without revealing the attribute to the proxy or the Cloud Service Providers.

Client Data privacy

Often, clients must protect data privacy before sharing the data. Consider an example in which multiple medical insurance companies, each of which has a designated Cloud Service Providers, would like to share customer data to have a much larger customer database from which to obtain useful statistical query results. One Cloud Service Providers might have an application that requires information on the percentage of male construction workers in the US who are younger than 40 and have respiratory diseases. This would require collecting data from multiple Cloud Service Providers for the analytical results to be meaningful, since the data from one Cloud Service Providers might be inadequate (after filtering for multiple selective predicates) or atypical (say, one Cloud Service Providers only has data for customers in a particular region of the US).

In this example, the disease attribute of records is sensitive and requires protection when shared among multiple Cloud Service Providers. Using encryption is not a viable option because maintaining the data's utility is a key requirement for many applications. Most applications require well-balanced tradeoffs between formal privacy and practical utility.

Privacy protection methods (other than encryption) fall broadly into two categories

Data perturbation (also known as input perturbation), which adds some form of noise to the data itself, and

Output perturbation, which adds noise to the otherwise accurate query answers.

V.CONCLUSIONS

This paper we discuss all those technique that are area of concern when a Linguistics is to be changed the shell or the architecture to built the environment, the platform on which the services are to be shared and at last the market point of view that is its cost effectiveness compared to the available. The multi-cloud environment can end the vendor lock-in of the consumer which is attained in the single cloud. The major area of concern in this field is the agreement between the cloud service providers for collaboration of their services in multi-cloud. The consumer will get highly benefited with multi-cloud environment and obtain service based on his preferences and requirement and not based on his cloud service provider. We proposed a framework that uses proxies to act as mediators between applications in multiple clouds that must share data. Our 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.

REFERENCES

[1] P. Mell and T. Grance, *The NIST Definition of Cloud Comput-ing*, special publication 800-145, Nat'l Inst. Standards and Technology, 2011, p. iii + 3.

[2] 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. 1-22,2012[2]

[3] P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory," Nat'l Inst. Standards and Technology, 2008; http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf

[4] R. Wu, G.J. Ahn, and H. Hu, "Towards HIPAA-Compliant Healthcare Systems," *Proc. 2nd ACM Int'l Symp. Health In-formatics* (IHI 12), ACM, 2012, pp. 593-602.

[5] N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," *ACM Com-puting Surveys*, Mar. 1989, pp. 515-556.

kediga pallavi, pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Narsimha Banothu, Associate Professor (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Janapati Venkata Krishna, Associate Professor & H O D (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.