An Intelligent Technique for Framework and Security Issues Association in Multi Cloud Environment

J Manjuvani [1], Bhaludra Raveendranadh Singh [2], K Laxmi [3], Moligi Sangeetha [4]

[1] *Pursuing M.Tech (CSE),* [2] *working as Principal,* [3] *working as Assistant Professor(CSE),* [4]*Associate professor & HOD (CSE)*
[1,2,3,4]*Visvesvaraya College of Engineering and Technology (VCET), M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D)-501510, India*

***Abstract*— Cloud Computing is a recent technology which rapidly developing in area of information technology has the concern of the network. It provides a huge change in technology that Internet based computing, by which software, information and shared resources are provided to computers and the strategy on demand, like the grid of the electricity. Cloud computing is the product of the synthesis of traditional computing technology and network technology like parallel computing, distributed computing. The main goal of cloud computing is to construct a perfect system with powerful computing capability through a large number of relatively low cost computing entity using the advanced business models like SaaS, PaaS, IaaS to distribute the powerful computing capability to end users. Developers, Administrators, and Users have to make a decision about which environment is best suited for them. When we trying to compare such frameworks it is difficult because either users do not have access to all of them or they are comparing the performance of such systems on different resources that make it difficult to obtain objective comparisons. Hence virtualization of resources such as memory, network, processors and storage ensures scalability and high availability of computing capability. However 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. The rapid provisioning and dynamic reconfiguration of resources help to handle with variable demand and ensure optimum resource utilization. Proposed proxy-based multicloud computing framework allows dynamic, resource sharing and on the fly collaborations among cloud based services, policy and privacy issues, and addressing trust without pre established collaboration agreements.**

Keywords: collaboration, cloud computing, security framework, service model, security challenges; security threats, resource virtualization.

I. INTRODUCTION

A Finite definition of Cloud Computing is "a system that is concerned with the calibration, virtualization, management, and integration of services and resources".

The benefits of cloud computing:

- Minimized Capital Expenditure
- Efficient utilization improvement
- High computing power
- Location and device independence and
- Very high scalability.

Cloud Computing provides following essential Features:

Broad network Access:

Availability of Capabilities through the network and accessed through standard mechanisms that promote use by heterogeneous wide client platforms.

On demand self service:

The end user can uniquely provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Rapid Elasticity:

Capabilities can be elastically provisioned and released in few cases automatically for scale rapidly outward and inward equal based on demand. The end user, capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service:

Cloud system automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of services. Resource usage can be watched, reported and controlled, providing transparency for both the provider and consumer of the utilized service.

Resource pooling:

The provider's computing resources are pooled to serve multiple consumers using a multi tenant model, by different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Location independence means that the customer generally has no

control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction.

Why Cloud Computing?

Cloud computing brings a new development in the field of Information Technology that gives a model where a user who wants to gain access to the software without licensing it, and need a platform to run this software and the infrastructure can access these services on pay-per-use basis. It also provides a large amount of data storage to the user who can utilize it and moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. We have approaches that encourage the owner to store the data, it offer some sort of guarantee related to the reliability, privacy and access control of the outsourced data. The u ser who gain access to the cloud service gain all these services but the user gets vendor lock-in and has to use all the service by this particular cloud service provider if users want to gain access to another cloud service provider for more effective and low cost management user has to authenticate to a particular service provider in this way user has to use multi service provider. By individual basis and pay separately for the service to each provider. Proposed scenario of multi-cloud presents a model called collaboration of multi-cloud where the user vendor lock-in can be abolished with an agreement between the various cloud service provider that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement and cost management.

In fig 1 it will illustrate contract with the peaks in service and resource requests using external ones, on demand basis, optimize costs or improve quality of services, react to changes of the offerts of the providers, follow the constraints, like new locations or laws, replicate the applications or services consuming resources or services from different Cloud providers to ensure their high availability, avoid the dependence on only one external provider, ensure backup-ups to deal with disasters or scheduled inactivity, act as intermediary, enhance own Cloud resource and service offers, based on agreements with other providers, consume different services for their particularities not provided elsewhere.

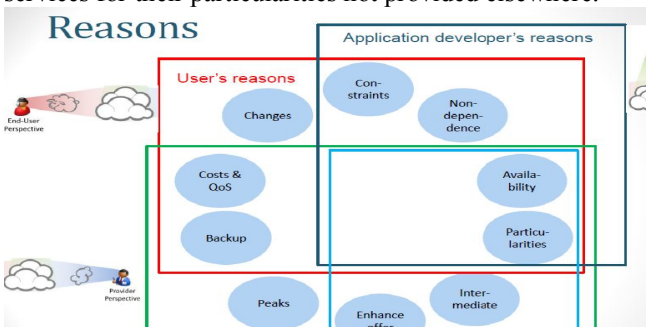

Fig 1: Reasons for using Cloud Computing

II. RELATED WORK

Existing cloud data services provide similar access control models so that individual and organizational privacy is a key requirement for iniquity management is unprotected. So the scope of insider terrorizations, a major source of data stealing and privacy breaches are no longer limited to the organizational perimeter. Hence multi cloud environments exacerbate these issues because proxies can access data client side. Illuminating sensitive information in uniqueness attributes to proxies that grant them authorization to access the data on behalf of clients is not an attractive solution.

The review of the systems which will be useful for moving from the single cloud structural planning to multi-cloud building design the security model and expense viability of multi-cloud contrasted with a cloud. Cloud computing has numerous favorable conditions; for example, it gives use of information from different cloud services, the capability of decision making for the client will stops vendor lock in and synchronization between distinctive cloud administration suppliers with expense advancement. 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" which detail the use of proxy at different levels of collaboration. So these proxies could be actualized by the cloud service provider or can be set by the institutions\organization in order to increase administration from the collaborated service providers. These alternatives can equally to be used to have a secure communication between the customer and the service provider. To protect stored data and data in transit and proxies must provide a trusted computing platform that keeps noxious programs from taking control and compromising sensitive customer and cloud requisition information.

Existing mechanisms and Policies & Problems:

Policy incongruities can result in security and availability problems; they include the following:

• *Redundancy:* The policy is terminated if every access request that matches the policy also matches another policy with the same effect.

• *Verbosity:* The similar to data element merging in data integration, policy composition can merge similar policies from different origins; resolving the policy verbosity during composition affects the policy size.

• *Contradiction*: Two policies are contradictory if they have different effects on the same subjects, conditions and targets. Contradictions are the most common form of policy conflicts.

• *Exception*: A policy is an exception of another policy if they have different effects, so one policy is a subset of the other. Exception might not be a policy conflict except access policy evaluation mechanisms commonly use exceptions to exclude a specific access request from general access permission

.

• *Correlation*: Two policies are correlated if they have different effects but intersect each other. With this policy permits the intersection to the other does not. This is a limited policy clash.

III. PROPOSED METHODOLOGIES

Our proposed framework for generic cloud collaboration allows clients and cloud applications to together use services from and route data among multiple clouds. Proposed framework supports common and dynamic collaboration in a multi cloud system. Then the entire clients are use services from multiple clouds without prior business agreements among the cloud providers, without suitable common values and provisions. Most of organizations obtain 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 service, possibly with on-premises (client-side) data and services. This service boundary 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, together transitional results process the combined data and produce final results.

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 availability, reliability and scalability. Multi cloud system that employs proxies for collaboration consists of three architectural components: multiple networks of proxies, cloud computing systems, 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 data amount they required to store for a particular time slice, without any apprehensions for efficient 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 runtime deployment. Researchers wishes 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 devided 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.

IV. PROXY BASED FRAMEWORK

A proposed proxy based multi cloud computing framework enables the dynamic on the fly collaborations and resource sharing among cloud is contingent services, reliable policy, and privacy problems 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 context the cloud service provider swarm 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 a separate cloud. The numerous 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:

The Proxy will also be interconnected 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. 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.

V. MULTI-CLOUD FRAMEWORK

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 difficulty vary, so we converted that a principled description of these services is needed to promote the interoperability and federation between heterogeneous cloud environments.

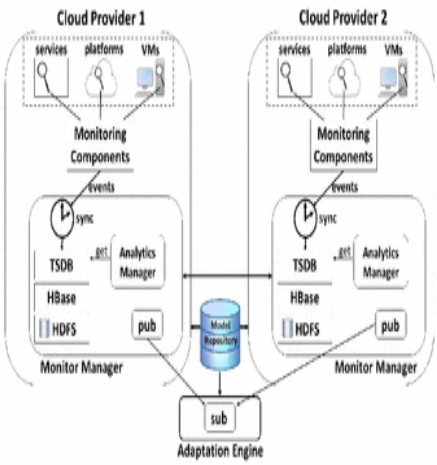

Fig 2: Multi Cloud Framework

This approach to building new collaborative services does not support flexibility, agility and openness. Multi cloud realizing collaboration's full potential will needs implicit, obvious, entire, and on-the-fly interaction involving different services spread across multiple clouds that lack pre established agreements.

The joined structure is based on the following three models:

Open Service Model

The disparate layers of a cloud environment provide dedicated services. However their granularity and difficulty vary, so the trust ness that a principled description of these services is needed to promote the interoperability and federation between heterogeneous cloud computing environments. The Service Component Architecture is intended for running a service based distributed applications. So it wills supports the communication between different protocols to this it has an idea of required. Since 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. The Software product line can be defined as a set of software intensive system that share a common set of features those are handled 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 specific cloud. The service list first allocated 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.

VI. IDENTITY ATTRIBUTES AND DATA PRIVACY

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

Identity attributes privacy

Data as a service (DaaS) 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 can specify access control policies on protected objects in terms of a subject's properties, called *identity attributes*. They can incorporate a subject's emailid, age, organizational role, and access location. Such an *attribute-based accessed 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 confidential information. The current cloud data services provides similar data access control models, in which separate and organizational confidentiality and key requirement for digital uniqueness management, is insecure.

In multicloud environments, where proxies use attribute based access control (ABAC) to retrieve client data from clouds, clients required to hide their uniqueness attributes from both proxies and Cloud Service Providers to preserve the privacy of sensitive client information. Hence clients must still give proxies the information that grants them access to requested data. Requirement calls for the use of identity attribute and data encoding techniques that permit oblivious data transfer between Cloud Service Providers, clients and proxies 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 encrypting, without having the client disclose its identity attributes to either entity. Identity

attribute and data encoding techniques must ensure that decoding the data is possible when the identity attributes match the attribute based access control policies without revealing the attribute to the proxy or the Cloud Service Providers.

Client Data privacy

Often, clients must protect data privacy before him sharing the data. For consideration take 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 infections. This would require collecting the 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 most of applications. Lot of applications needs well-balanced tradeoffs between formal privacy and practical utility.

Privacy protection methods broadly divides into two categories

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

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. Cloud computing is new and rising very quickly, but because security problems are still delaying its adoption so we need to provide security mechanisms to ensure that cloud computing benefits are fully utilized and realized. While there are many benefits to using a cloud based system and practical problems remain that have to be solved before the technology can be more fully deployed and particularly those problems related to service level agreements, security, privacy, and power productivity. Proposed framework contains refining the proxy deployment scenarios and development of infrastructural and operational components of a multi cloud system. Proposed scenario accompanied by implementation of an experimental platform using open source tools and libraries.
Enhance id management protocol framework for more verification. The user centric uniqueness management and is being considered as a complete all-round solution addressing all possible issues of cloud IDMs.

References

[1] Mukesh Singhal And Santosh Chandrasekhar, Merced Tingjian Ge, Ravi Sandhu And Ram Krishnan, Gail-Joon Ahn, Elisa Bertino – "Collaboration In Multicloud Computing Environments: Framework And Security Issues" On IEEE Transactions On Cloud Computing Vol:46 No:2 Year 2013.

[2] International Journal On Cloud Computing: Services And Architecture (Ijccsa), Vol.2, No.1, February 2012 Doi : 10.5121/Ijccsa.2012.2101 1 Enhancing The Security Framework Securecloud With The Swift Identity Management Framework

[3] 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.

[4] 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.

[5] R. Thandeeswaran, S. Subhashini , N. Jeyanthi1, M. A. Saleem Durai, "Secured Multi-Cloud Virtual Infrastructure with Improved Performance", cybernetics and information technologies XII.

AUTHOR PROFILE

Ms. J.Manjuvani is currently pursuing M.Tech in the Department of Computer Science & Engineering, Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy(D), India. Her research interests include Network Security.

Sri Dr. Bhaludra Raveendranadh Singh working as Associate Professor & Principal in Visvesvaraya College of Engineering and Technology obtained M.Tech, Ph.D(CSE)., is a young, decent, dynamic Renowned Educationist and Eminent Academician, has overall 20 years of teaching experience in different capacities. He is a life member of CSI, ISTE and also a member of IEEE (USA).

Ms. K.Laxmi working as Asst. Professor (CSE) in Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy(D), India.

Ms's. Sangeetha M working as Assoc. Professor & HOD (CSE). She has completed bachelor of technology from Swamy Ramananda Theertha Institute of Science & Technology and Post-graduation from Jawaharlal Nehru Technological University,Kakinada campus and is having 12 years of teaching experience.