A Review on Data Storage in Multi-Cloud Environment for Privacy Preserving

D.Suman[1], Dr. K. Babu Rao[2]

[1]Prasad Engineering College, Jangaon, Telangana, India.

[2]Prasad Engineering College, Jangaon, Telangana, India.

Abstract- **Cloud computing provides a service based on internet for several shared resources and system software across various environment. For secure cloud storage the process of encryption of the data to the users for various needs has been brought by the delegated access control method. Generally storage in public cloud requires high communication, heavy load due to maximum storage and high computational costs. In this paper, we are implementing multi-cloud environment for secure storage where it acts as a public cloud and provides low costs, also it involves two- layer encryption over the data stored in the cloud. We are using an efficient AES algorithm which provides higher confidentiality and privacy for several users in the cloud and stores the data in multi-clouds where the users can retrieve with the keys later while delegating it through access control from the cloud. Security and cost are the top issues in this field and they vary greatly, depending on the vendor one choose.**

Index Terms- **Privacy, Cloud Computing, Delegation, Encryption, Access Control.**

I. INTRODUCTION

A. Cloud computing

Cloud computing is everywhere because the locality of physical resources and devices has been accessed in general are not known to the end user. It also provides services for users to build deploy and manage their applications on the cloud. It involves virtualization of resources that maintains and manages by itself. It is a tool for providing simple, needed network access to a shared resource of configurable computing environment (network, storage etc) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Today most of the companies have to process huge amounts of data in a cost- reducing manner. Classic users are operators of Internet search engines such as Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made database solutions more expensive.

B. Privacy and Security

Security is mainly necessary for strong privacy in all online computing factors, but security alone is not enough. Security and cost are the top issues in this field and they vary greatly, depending on the vendor one choose. Despite the first success and recognition of the cloud computing model and the extensive availability of providers and tools, a number of challenges and risks are innate to this new model of computing.

C. Delegation

Data collector may share data with unknown parties if they do not follow the privacy policy. In the proposed model, delegation follows privacy policy which allows only legitimate parties accessing the data. It also sets the data usage guidelines for them. Between two parties as inter-visibility delegation. The party or visibility which shares data is called source visibility while the visibility that receives data is called destination visibility. In addition, we study intra-visibility delegation where two users within a party share the access rights with each other. Users who delegate the rights are called delegators while users who receive the rights are called delegates.

II. COLLABORATION FRAMEWORK FOR MULTICLOUD SYSTEMS

Our proposed collaborative generic cloud framework allows clients and cloud applications to use services from and route between multiple clouds simultaneously. This framework promotes universal and dynamic collaboration in a multicloud system. It allows clients simultaneously use multiple cloud services without preceding trade agreements between cloud providers, without the adoption of common standards and specifications.

A. Use of proxies for collaboration

In the current context, a client who wishes concurrently use multiple cloud services should interact individually with every cloud service, collect intermediate results, the treatment group data, and generate the final results. The following constraints in the model of cloud computing today prevent direct collaboration among applications different cloud hosted applications:

B. Heterogeneity and Tight Coupling

Clouds realize proprietary interfaces for service access, configuration, and organization as well as for interaction with other cloud components. Each service layer of a cloud strongly integrates with lower service layers or is highly dependent on the value-added proprietary solutions that the cloud offer. This heterogeneity and tight coupling prohibit interoperation between services from different clouds.

1. Pre-Established Business Agreements: The current business model requires pre-established agreements between CSPs before collaboration can happen. These agreements are essential for clouds to determine their willingness to collaborate and build trust with each other. The absence of such agreements prohibited multi-cloud cooperation because of incompatible intentions, business rules and policies. In addition, collaborations under pre-established agreements generally have a tight integration between the participants and cannot be extended to provide a universal and dynamic collaboration.

2. Service delivery model: Clouds use a service delivery model that provides service access to legitimate subscribing clients and denies all other requests because of security and privacy concerns. This prevents direct communication between services from different clouds. Also, CSPs typically package their service offerings with other resources and services. This results in a tight dependency of a service on the hosting CSP. Such examination delivery model limits a client’s ability to customize a service and use it in combination with service offerings from different CSPs.

A technique that could overcome these limitations using a network of proxies. A surrogate is an edge-node-hosted software instance that a client or CSP can delegate to perform operations on its behalf. Depending on the context, the system can consider a network of proxies as a collection of virtual connected via a virtual network or set of software instances physical nodes connected via an infrastructure of the underlying network. The basic idea is to allow proxies acting on behalf of a subscribing client or a cloud to provide a diverse set of functionalities: cloud service interaction on behalf of a client, the data processing using a rich set of operations, caching intermediate results, and routing, among others. With these additional functionalities, proxies can act as intermediaries for collaboration among the services on different clouds. Proxy deployment can be strategic - in close geographical proximity in the clouds, for example, to improve performance and facilitate the implementation of long lived applications without additional user intervention.

As an example of proxy facilitated collaboration between clouds, regard as a case in which a client or CSP wishes simultaneously use a set of services that offer multiple clouds. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications. A client or CSP could use several proxies to interact with several DSP. It can be selected on the basis of proxies, for example, latencies between the proxies and the clouds or conditions workload to different agents. Once it chooses proxies, the client or CSP delegates the necessary service-specific privileges to the proxies to carry out the service request using the necessary security precautions. These proxies can extra delegate to other proxies if necessary and initiate the service request.

In some instances, clients or CSPs can assign special roles to one or more proxies in the network to coordinate the operations in a service request among the multiple delegate proxies. Following delegation, the requesting entity need not further interact with the proxy network until the proxies complete the service request. During the execution of a service request, the proxy will interact with applications based on cloud, playing the role of the subscriber (s) of service. By independently requesting services from the clouds and data routing them in a transparent manner for cloud applications, proxies can facilitate collaboration without requiring prior agreements between the CSPs. Proxies can also perform operations to help overcome incompatibilities among services to allow the exchange of data between them.

C. Architectural overview

Clouds are made up of several groups of resources connected to the network, such as server farms, data warehouses, and so on that host virtual machines distributed geographically and storage components that provide the scalability, reliability, and high availability. A multi-cloud system that utilizes proxies for collaboration consists of three architectural components: multiple cloud systems, networks of proxies, and clients (or users of services). Such systems can use several possible strategies for placing proxies in the proxy network.

1. Cloud-hosted proxy: As Fig.1 shows, each CSP can host proxies within its cloud infrastructure, manage all proxies within its administrative domain, and handle service requests from clients that wish to use those proxies for collaboration. The proxy instances might need to be CSP specific. For example, in Fig.1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains.

2. Proxy as a service: As Fig.2 shows, this scenario involves deploying proxies as an autonomous cloud that offers collaborative services to clients and CSPs. A group of CSPs that are willing to collaborate can manage this proxy-as-a-service cloud, or a third-party entity, a proxy service provider (PSP), can provide management. Clients directly subscribe to the proxy cloud service and employ them for inter cloud collaboration.

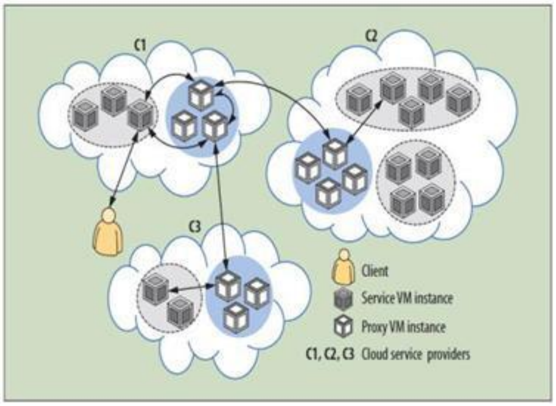

Fig.1. Client sends a request to cloud C1, which dynamically discovers the need to use services from clouds C2 and C3. C1 employs proxies to manage these interactions.

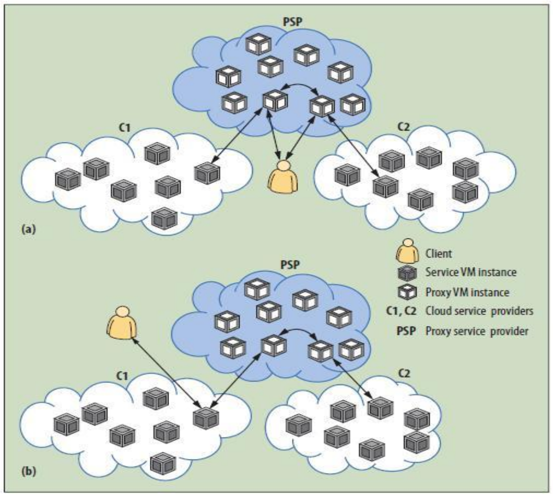

Fig.2. Proxy as a service. In this scenario, cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients. (a) A client employs two proxies to interact with CSPs C1 and C2. (b) Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2. PSP: proxy service provider.

3. Peer-to-peer proxy: Proxies may also interact in a peer-to-peer network is managed by either a PSP or a group of CSPs who wish to collaborate. Another possibility is of proxies do not have the collective management: every proxy in the peer-to-peer network is an independent entity that manages itself. In this case, the proxy itself must handle requests for utilize of its services.

4. On-premise proxy: In the scenario shown in Fig.3, a client can host proxies within its organization's infrastructure (or on premises) and manage all proxies within its administrative domain. A client that wishes to use proxies for collaboration will employ its on-premises proxies, whereas CSPs that wish to collaborate with other CSPs must employ proxies that are within the domain of the service-requesting client.

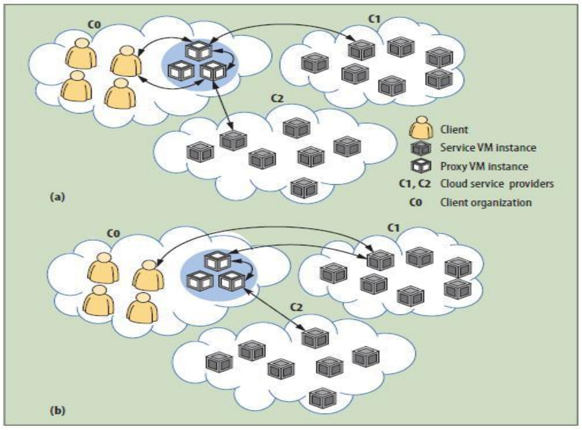

Fig.3. On-premises proxy. Clients deploy proxies within the infrastructure of their organization. (a) A client employs two proxies to interact with CSPs C1 and C2. (b) A client initiates a service request with C1, which then discovers the need for a service from C2.

5. Hybrid Proxy Infrastructure: A hybrid infrastructure can include on-premises, CSP- and PSP-maintained, and peer to peer proxies. Selecting proxies for collaboration will depend on the type of service being requested and the entity that initiates collaboration, among other factors. For example, clients that must initiate a service request with two CSPs can employ on-premises proxies for collaboration. On the other hand, a cloud-based application that discovers it needs a service from another CSP to fulfill a client's request can employ a CSP-maintained proxy. The proposed architectures illustrate the various options that are available for deploying proxies to support collaboration. Developing these architectures serves as the first step in building a proxy-based, collaborative, multi-cloud computing environment.

A complete solution will require several additional tasks. For instance, an important task is a comprehensive study and evaluation of architectures based on proxies proposed. Such an evaluation should cover possible variations of each architecture in various cases and collaboration scenarios multi-cloud practical use. Based on this study, researchers can refine the proposed architectures, develop new variations to support different scenarios and use cases, and, if possible, merge architectures in an architecture-based universal proxy multi-cloud cooperation. Another important task is to develop a full range of protocols and mechanisms that proxies must implement to support all the functionalities needed to act as mediators among the services of several clouds. For instance, support collaboration scenarios that migrates a client-subscribed virtual machine from one cloud to another require technical translation between packets of the virtual machine and distribution formats.

III. SECURITY ISSUES IN MULTICLOUD COLLABORATION

Researchers and industry specialists have highlighted several security issues in cloud computing, including isolation management, data exposure and confidentiality, virtual OS security, trust and compliance, and mission assurance.8 Specific security issues emerge during dynamic sharing and collaboration across multiple clouds. In particular, issues pertaining to trust, policy, and privacy are a concern in multi-cloud computing environments.

A. Establishing trust and safe delegation

As in other IT systems, security in the cloud relies heavily on the establishment of trust relationships among involved entities. The need for trust happens because a client abandons the direct control of the security and privacy of its assets to a CSP. This exposes a client's assets to new risks that are preventable or decreased in internal organization. These risks include internal security threats, weakening the rights of ownership of data, transitive trust issues with third party providers of cloud services composites, and decrease system security surveillance. A customer must confer a high level of confidence in a CSP regarding its ability to implement effective controls and processes to protect property. Thus, a client must be able to accept higher levels of risk in the use of cloud-based services. Utilizing proxies moves the trust boundary one step further: clients and CSPs now must establish trust relationships with the proxies, which comprises security of accepting a proxy's security, reliability, availability, and guarantees business continuity of a proxy.

In addition, the CSPs responding to service requests that a proxy makes on behalf of a client or another CSP must trust the proxy to legitimately act on behalf of requesting entity. Establishing a relationship of trust with the proxies depends on the strategy used to create, manage and administer the network proxy. The entity managing proxies shall provide guarantees reliable operation of its own; in addition, it must provide guarantees of safety, reliability and availability of proxies.

From the client's point of view, employing on-premises proxy that is within the client's administrative domain can exacerbate trust issues. By using on-premises proxy, a client maintains control over its assets while proxies process them during a collaborative service request. Similarly, using proxy within the CSP's administrative domain lets the CSP implement control over the proxies' operations, and thus it can trust the proxies to enable collaboration.

Proxy networks are a potential platform for the development of architectures and solutions for systems based proxy's multi-cloud security. At a minimum, the network of proxy must implement security mechanisms and privacy mechanisms that mirror, expand or complement similar mechanisms offered by clouds8 to maintain protection of assets outside the realm of clouds and client organizations. For instance, to protect data at rest and data in transit, proxies must provide a computing platform of trust that prevents malware to take control and compromise customer data and sensitive applications cloud. They must also ensure the confidentiality and integrity of data during transmission across the network proxy, optionally using standards such as the security protocol of the transport layer.

IV. CONCLUSION

In this paper, we present a unique method for privacy preserving of data storage in multi-cloud environment. It also provides several advancements in cloud computing due to its technical capabilities. The feature work may also involve load-balancing in multi-cloud environment for maximum storage and accuracy for various users. Cloud computing is a growing paradigm as an enabling technology to deliver on-demand and elastic storage and computing capabilities, while removing the ownership need for hardware. But several privacy and security act demand strong protection of the cloud users, which in turn increases the complexity to develop privacy-preserving cloud services. The privacy preserving using delegated access control in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

V. REFERENCES

[1] M.Newlin Rajkumar, P.M.Benson Mansingh, Dr.V. Venkatesa kumar, "An Efficient and Secure Storage Using Delegated Access Control in Multi-Cloud Environment", Volume 1, Issue 4 December 2013.

[2] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEE International Conference on Information Reuse and Integration (IRI), 2012.

[3] Rakshit, A. , et. Al, "Cloud Security Issues", 2009, IEEE International Conference on Services Computing

[4] M.S.B. Pridviraju et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5), 2012,5206 – 5209.

[5] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM Trans. Inf. Syst. Secur., vol. 5, no. 3, pp. 290–331, 2002.

[6] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in VLDB '2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003, pp. 898–909.

[7] N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A privacy- preserving approach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[8] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based roxy re-encryption with delegating capabilities,” in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS ’09. New York, NY, USA: ACM, 2009, pp. 276–286.

[9] C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng, “Conditional proxy broadcast re-encryption,” in Proceedings of the 14th Australasian Conference on Information Security and Privacy, 2009, pp. 327–342.

[10] J.-M. Do, Y.-J. Song, and N. Park, “Attribute based proxy reencryption for data confidentiality in cloud computing environments,” in Proceedings of the 1st International conference on Computers, Networks, Systems and Industrial Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2011, pp. 248–251.

[11] L. Bussard, G. Neven and F.S. Preiss, “Downstream Usage Control,” In proceedings of 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 22-29, 2010.