ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, S.Iss 6, 2022

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

[1]Shail Dubey, [2]Pooja Diwivedi, [3]Ashish Shukla, [4]Rituraj Kushwaha, [5]Abhay Shukla, [6]Shalini Gupta

Deaprtment of Computer Applications, Axis Institute of Higher Education, Kanpur, Uttar Pradesh, India

Abstract

Cloud computing offers an online solution for multiple shared resources and system software in different environments. The delegated access control approach has introduced the practice of encrypting user data for a variety of purposes, ensuring secure cloud storage. Because of the greatest storage capacity and high computational expenses, public cloud storage typically necessitates high connectivity and significant load. This study presents the implementation of a multi-cloud environment for safe data storage that offers low-cost public cloud services along with two-layer encryption over cloud data. We store the data in multiple clouds where the customers can access it more privately and confidentially thanks to our effective AES algorithm.

Index Terms- Access control, encryption, delegation, privacy, and cloud computing.

I. OVERVIEW

A. Cloud-based computing

Since the end user typically doesn't know where the actual resources and devices that have been accessed are located,

Cloud computing is pervasive. Additionally, it offers services that let customers create, launch, and maintain cloud-based apps. It entails visualizing self-maintained and self-managing resources. It is a tool that enables quick provisioning and release of shared resources inside a re-configurable computing environment (network, storage, etc.) with little management work or service provider contact. The majority of businesses nowadays must process massive volumes of data in an economical way.Operators of Internet search engines like Microsoft, Yahoo, and Google are considered classic users. The sheer volume of data they handle on a daily basis has driven up the cost of database solutions.

B. Privacy and Security

Strong privacy in all aspects of online computing primarily depends on security, yet security by itself is insufficient. The most important factors in this industry are security and pricing, which might differ substantially depending on the vendor selected. Despite the cloud computing model's initial success, recognition, and wide despite the accessibility of resources and instruments, there remain certain inherent risks and constraints associated with this new computing paradigm.

C.Delegation:

If data collectors disregard the privacy rules, they could disclose data to unidentified parties. Delegation under the suggested model complies with privacy policies, granting access to data

only to authorised parties. It also establishes their criteria for using data. as a delegation of inter-visibility between two parties. Source visibility refers to the party or visibility that distributes data, and destination visibility refers to the visibility that receives data. Furthermore, we examine the concept of intra-visibility delegation: this is the trade of access rights between two users in the same party.

those who receive privileges are referred to as delegates, and those who delegate rights are known as delegators.

I. COLLABORATION FRAMEWORK FOR MULTICLOUD SYSTEMS

Cloud apps and clients can move between clouds and obtain services from them at the same time with our collaborative generic cloud architecture. This architecture facilitates dynamic and universal cooperation in a multiload system. In the absence of previous trade agreements between cloud service providers and the creation of uniform guidelines and requirements, it enables clients to use numerous cloud services simultaneously.

A. Use of proxies for collaboration

A client who wants to use many cloud services at the same time in the current context should communicate directly Compile treatment group data, provide intermediate findings, and generate final results for each cloud service. The following constraints in the cloud computing model currently restrict apps housed on different clouds from communicating directly with one another:

B.Tight Coupling and Heterogeneity

Clouds realize proprietary interfaces for service access, configuration, and organization, in addition to facilitating communication with other cloud components. Each cloud service tier is either highly reliant on the cloud's value-added proprietary solutions or has strong integrations with lower service layers. Interoperability between services from multiple clouds is prohibited by this heterogeneity and strong coupling.

Pre-Established Business Agreements: 1. The present business model precludes collaboration between CSPs unless pre-established agreements are made. Clouds need these agreements to assess each other's desire to work together and develop mutual trust. Due to conflicting goals, corporate regulations, and policies, multi-cloud collaboration was not possible in the absence of such agreements. Furthermore, pre-established agreements sometimes require close integration between the participants in partnerships, meaning that such collaborations cannot be expanded to foster a universal or dynamic one.

Service delivery paradigm: Because of security and privacy concerns, clouds use a service delivery paradigm that grants service access to clients who have legitimately subscribed while rejecting all other requests. This stops services from different clouds from communicating directly with one another. Moreover, CSPs frequently combine additional resources and services with their service offerings. As a result, a service becomes very dependent on the hosting CSP. This type of examination distribution model limits a customer's capacity to combine and match services from several CSPs and personalise their experience.

A method that would use a network of proxies to get around these restrictions. A client or CSP can designate a surrogate, This is a software instance hosted on an edge node, to do tasks on its

behalf. A network of proxies may be seen by the system as a collection of virtual nodes linked by a virtual network or as a set of physical nodes connected by the architecture of an underlying network, depending on the circumstances. The fundamental idea is to allow proxies acting on behalf of a cloud or a client that has subscribed to the service to provide a wide range of activities, such as data processing using a rich set of operations, routing, caching intermediate results, and client-side cloud service interaction. Proxy servers can serve as a bridge between services on various clouds to facilitate collaboration thanks to these extra features. Proxy deployment can be strategically placed in clouds, for example, to enhance performance and make it easier to develop long-lasting applications without requiring further user engagement.

As an illustration of proxy-facilitated cloud cooperation, consider the scenario when a customer or CSP desires to utilize several services offered simultaneously by several clouds. The asking entity first selects proxy to communicate with cloud apps and act on its behalf. Multiple proxies could be used by a client or CSP to communicate with multiple DSP. It can be chosen based on proxies, factors affecting the burden to various agents, or latencies between the proxies and the clouds. After selecting proxies, the client or CSP grants the proxies the authority to perform the service request while taking the required security measures. If additional delegation is required, these proxies can start the service request and assign it to other proxies.

To synchronize the actions of several delegate proxies in a service request, clients or CSPs may assign specific tasks to one or more network proxies under specific circumstances. Following delegation, up until the proxies provide the requested service, the requesting entity does not need to communicate with the proxy network again. The proxy will interact with cloud-based apps while a service request is being executed, taking on the role of the service subscriber or subscribers. Proxy servers enable cooperation between cloud service providers (CSPs) without the need for previous agreements by autonomously seeking services from the clouds and transparently data routing them for cloud applications. Additionally, proxies can help resolve service incompatibilities so that data can be sent between them.

B. Architectural overview

The several resource groups that comprise clouds include server farms, data warehouses, and other network-connected resource groups that house geographically dispersed virtual machines and storage components that enable scalability, reliability, and high availability. Proxies are used in a multi-cloud system to facilitate collaboration between three architectural components: networks of proxies, clients (or service users), and several cloud systems. These systems have a variety of options on how to arrange proxies within the proxy network.

1. **Cloud-hosted proxy:** Any cloud service provider (CSP) can host proxies on its cloud infrastructure, maintain control over all proxies within its administrative domain, and reply to service requests from clients that want to use those proxies for collaboration, as shown in Figure 1. It's possible that CSP-specific proxy instances are required. For example, in Fig. 1, C1 and C2 may mutually and dynamically provide sharing and collaboration logic as proxy virtual instances within their respective administrative domains.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, S.Iss 6, 2022

2. Proxy as a service: In this scenario, proxies are deployed as an autonomous cloud that provides clients and CSPs with collaborative services, as seen in Figure 2. This proxy-as-a-service cloud can be managed by an association of cooperative CSPs, or by an outside organization called a proxy service provider (PSP). Direct subscriptions to the proxy cloud service are made by clients, who use them for inter-cloud cooperation.

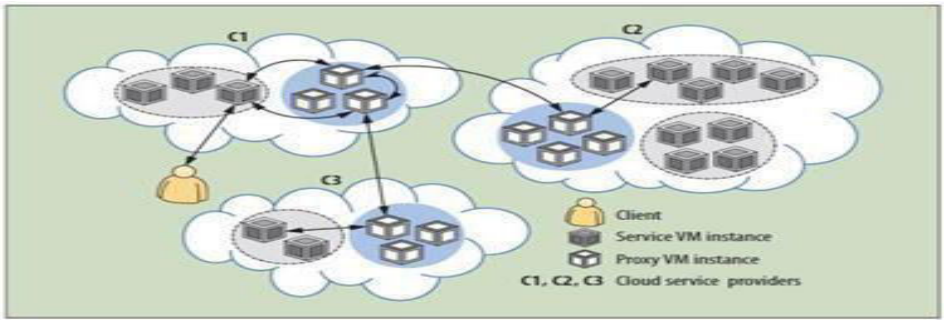

Fig.1. After receiving a request from the client, cloud C1 dynamically determines that services from clouds C2 and C3 are required. To handle these interactions, C1 makes use of proxies.

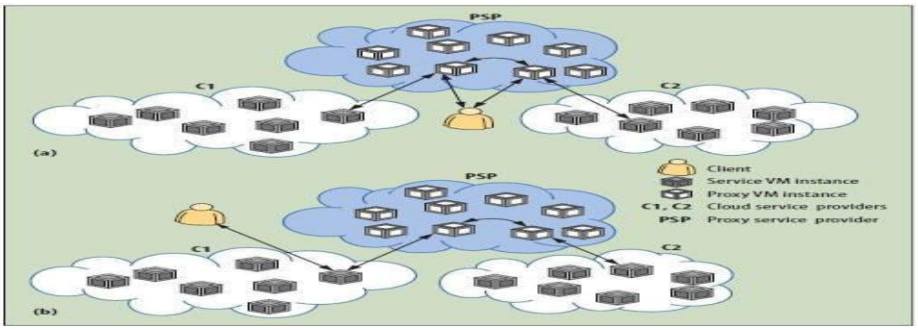

Fig.2. The use of proxies as services. In this case, proxies are set up by cloud service providers (CSPs) as an independent cloud system that they deliver to customers as a service. (A) A client communicates with CSPs C1 and C2 through two proxies. (a) As an alternative, a client contacts C1 to start a service request, and C1 subsequently determines that C2 can provide the necessary service. Proxy service provider, or PSP.

1.Peer-to-peer proxy: Furthermore, proxies can interact with one another in a peer-to-peer network managed collaboratively by CSPs or a PSP. Another scenario is that proxies do not have collective administration; rather, each proxy in a peer-to-peer network functions as a separate, self-governing entity. In this scenario, requests to use the proxy's services must be handled by the proxy itself.

On-premise proxy: In the scenario shown in Figure 3, a customer can host proxies on-site or within the infrastructure of its business. Additionally, within its administrative domain, it has control over all proxies. Clients that choose to use proxies for cooperation will use their on-premises proxies, while CSPs that wish to collaborate with other CSPs must use proxies that are within the domain of the service-requesting client.

Hybrid Proxy Infrastructure: Peer-to-peer proxies, CSP and PSP maintained, and on-premises systems can all be a part of a hybrid infrastructure. The choice of proxies for collaboration will be based on a number of factors, including the kind of service being sought and the party initiating the collaboration. For instance, clients can work together by using on-premise proxies when they need to start a service request with two CSPs. Conversely, a cloud-based application may use a CSP-maintained proxy if it finds that it requires a service from an additional CSP in order to handle a customer's request. The suggested architectures serve as examples of the several ways that proxies might be deployed to facilitate cooperation. Creating these architectures is the first step towards creating a collaborative, multi-cloud, proxy-based computing environment.

Several more chores will be necessary to provide a complete solution. For example, a thorough analysis and assessment of architectures based on suggested proxies is a crucial effort. Such an assessment ought to address potential modifications of every architecture in diverse scenarios and cooperative work environments including several clouds. Researchers can improve the suggested designs based on this study, create new versions to accommodate various use cases and circumstances, and, if feasible, combine architectures to create an architecture-based universal proxy collaboration across several clouds. Creating a comprehensive set Another critical challenge is determining what protocols and techniques proxies must employ to offer all the capabilities needed to function as mediators between the services of many clouds. For example, to enable cooperative scenarios involving the transfer of a client-subscribed virtual machine from one cloud to another, technical translation between virtual machine packets and distribution formats is required.

II. SECURITY ISSUES IN MULTICLOUD COLLABORATION

A number of security concerns related to cloud computing have been brought to light by researchers and industry experts. These concerns include trust and compliance, mission assurance, virtual OS security, data exposure and confidentiality, isolation management, and compliance.8 During dynamic sharing and collaboration across many clouds, specific security risks surface. In multi-cloud computing settings, trust, policy, and privacy concerns are particularly significant.

A. Establishing trust and safe delegation

Similar to other IT systems, cloud security is largely dependent on the development of relationships of trust between the various parties involved. When a customer gives up direct control over the security and privacy of its assets to a CSP, trust becomes necessary. This exposes the assets of a client to additional dangers that can be avoided or minimised throughout the business. These risks include decreasing data ownership rights, threats to internal security, issues with transitive trust with third-party cloud service providers, and a decrease in system security monitoring.

A customer must have complete faith in a CSP's ability to put in place efficient procedures and controls to safeguard assets. Because of this, using cloud-based services requires a client to be willing to assume greater degrees of risk. By By using proxies, clients and CSPs are required to

establish trust relationships with the proxies, which comprise guarantees of a proxy's availability, dependability, and security along with assurances of its business continuity. This extends the trust boundary.

A proxy's ability to operate lawfully on behalf of the requesting entity must also be trusted by the CSPs answering to service requests made by the proxy on behalf of a client or another CSP. The method employed to design, oversee, and maintain the network proxy will determine whether or not a trustworthy connection can be built with the proxies. The organisation in charge of proxies must assure not only the smooth functioning of its own operations but also the availability, safety, and dependability of the proxies.

Using an on-premises proxy that is located within the client's administrative domain may make trust difficulties worse, according to the customer. A client can execute its assets during a collaborative service request while still keeping control over them by utilising an on-premises proxy. Comparably, by utilising proxies inside the CSP's administrative domain, the CSP is able to exert control over the proxies' activities and, as a result, may rely on the proxies to facilitate cooperation.

Proxy networks offer a promising foundation for the creation of multi-cloud security architectures and solutions for systems-based proxies. To preserve asset protection outside the domain of clouds and client organisations, the network of proxies must, at the very least, incorporate security and privacy mechanisms that replicate, extend, or enhance comparable methods provided by clouds8. For example, proxies need to offer a computing platform of trust that stops malware from taking over and compromising client data and sensitive apps in the cloud in order to safeguard data both in transit and at rest. They must also use standards like the transport layer security protocol, if applicable, to guarantee the secrecy and integrity of data while it is being transmitted across the network proxy.

III. CONCLUSION

In this research, we describe a novel approach to data storage privacy preservation in a multi-cloud setting. Because of its technological capabilities, it also offers a number of breakthroughs in cloud computing. In order to maximise storage and accuracy for different users, load balancing in a multi-cloud environment may also be part of the feature work. A new paradigm in technology that makes it possible to provide elastic and on-demand computation and storage without requiring hardware ownership is cloud computing. However, a number of security and privacy laws require strict protection for cloud users, which makes it more difficult to provide cloud services that secure users' private. Delegated access control in multi-cloud privacy preservation offers the essential features needed for a reliable, affordable, and secure cloud security deployment.

IV. 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.