

Protecting Multiple Cloud System using Inter Cloud Concepts

D.Saravanan

Faculty of Operations & IT
ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.

Abstract

“Intercloud security considerations” framework for 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. The basic idea is to enable proxies that act on behalf of a subscribing client or a cloud to provide a diverse set of functionalities. With these functionalities, proxies can act as mediators for collaboration among services on different clouds. When proxies enable dynamic collaboration between multiple CSPs, heterogeneous security policies can be the source of policy conflicts that result in security breaches. Even though ‘existing’ policy evaluation mechanisms can verify individual domain policies, security violations can easily occur during integration. A policy integration process for intercloud collaboration must systematically handle potential conflicts and resolution problems. In proposed cloud collaboration allows client and cloud applications to use services from and route data among multiple clouds. Multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

Keywords - Cloud Computing, Inter cloud Collaboration, Security, Service providers, Multiple Clouds.

I. INTRODUCTION

A. Cloud computing

Cloud computing arises from its ability to provide software, infrastructure, and platform services without requiring large investments or expenses to manage and operate them. Clouds typically involve service providers, infrastructure/resource providers, and service users. As figure 1 shows, the “cloud” in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service.

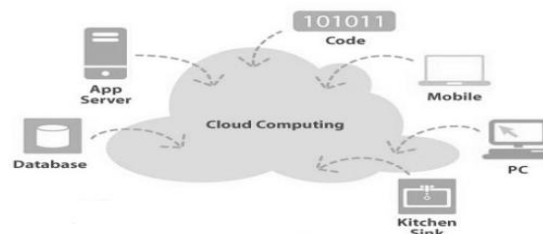


Fig. 1. cloud computing

B. Cloud service provider

Cloud service providers (CSPs) are developing new technologies to enhance the cloud’s capabilities. Cloud mashups are a recent trend; mashups combine services from multiple clouds into a single service or application, possibly with on-premises data and services. Realizing multi cloud collaboration’s full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services spread across multiple clouds that lack pre-established agreements and proprietary collaboration tools.

Mechanisms for collaboration across multiple clouds must undergo a rigorous, in-depth security analysis to identify new threats and concerns resulting from collaboration. They must have support of innovative, systematic, and usable mechanisms that provide effective security for data and applications.

Some specific security issues associated with collaboration among heterogeneous clouds include:

- establishing trust among different cloud providers to encourage collaboration;
- addressing policy heterogeneity among multiple clouds so that composite services will include effective monitoring of policy anomalies to minimize security breaches; and
- maintaining privacy of data and identity during collaboration.

C. Collaboration for Multicloud Systems

A proposed proxy-based multi cloud computing framework allows dynamic, on-the-fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without pre-established collaboration agreements or standardized interfaces.

D. Usage of proxies for collaboration:

In the current environment, a client that wishes to use services from multiple clouds must individually interact with each cloud service, gather intermediate results, process the collective data, and generate final results. Proxies can facilitate collaboration without prior agreements between the cloud service providers. A proxy 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 proxies as a collection of virtual software instances connected via a virtual network or a set of physical nodes connects via an underlying network infrastructure. During execution of a service request, proxies would interact with cloud-based applications, playing the role of the service subscriber. Proxies can also perform operations to help incompatibilities among services to allow data exchange between them.

II. ARCHITECTURE OF MULTI CLOUD ENVIRONMENT

A multi cloud system that employs proxies for collaboration consists of three architectural components: Multiple cloud computing systems, networks of proxies, and clients.

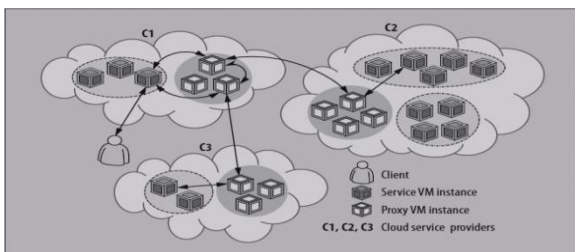
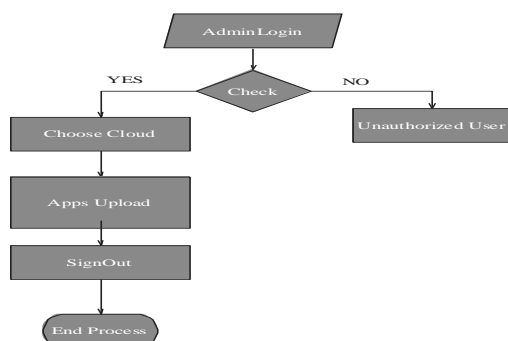


Fig. 2..Multi cloud Environment

A. Cloud-hosted proxy

As Figure 2 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 Figure 1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains. Client sends a request to cloud C1, which



dynamically discovers the need to use services from clouds C2 and C3. C1 employs Fig. 3. Proxies to manage these interactions.

B. Proxy as a service

As figure 3 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. Cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients. A client employs two proxies to interact with CSPs C1 and C2. Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2. PSP: proxy service provider.

III. ATTRIBUTE-BASED ACCESS CONTROL

Developing proposed architecture serves as the first step in building a proxy-based, collaborative, multi cloud computing environment. Proxies must implement to support all the functionalities necessary for acting as mediators among services from multiple clouds. Proxy networks are a potential platform for developing proxy-based security architectures and solutions for multi cloud systems. To protect data at rest and data in transit, proxies must provide a trusted computing platform that prevents malicious software from taking control and compromising sensitive client and cloud application data.

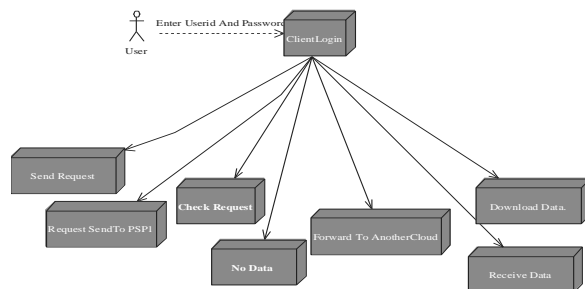


Fig. 4. Multicloud transaction

An expressive access control model can specify access control policies on protected objects in terms of a subject's properties, called identity attributes. 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. 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. Multi cloud environments exacerbate these issues because proxies can access data on behalf of clients. Revealing 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, assuring the private and consistent management of information relevant to ABAC becomes more complex in multi cloudsystems. Inmulti cloud environments, where proxies use ABAC to retrieve client data from the clouds, clients need to hide their identity attributes from both proxies and CSPs to preserve the privacy of sensitive client information.

IV. EXPERIMENTAL SETUP

A .Collaboration framework for Multi cloud system Module

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 use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

B. Client/Users Module

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. A client that wishes to use services from multiple clouds must individually interact with each cloud service, gather intermediate results, process the collective data, and generate final results. Proxies can facilitate collaboration without requiring prior agreements between the cloud service providers. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications. A client or a CSP might employ multiple proxies to interact with multiple CSPs. It can select proxies based on, for example, latencies between proxies and clouds or workload conditions at various proxies.

C. Cloud service providers

Cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients. A client employs two proxies to interact with CSPs C1 and C2. Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2.

D. Proxy service provider

Clients deploy proxies within the infrastructure of their organization. A client employs two proxies to interact with CSPs C1 and C2. A client initiates a

service request with C1, which then discovers the need for a service from C2.

E .Proxy Service Provider

It 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 intercloud collaboration. To protect data at rest and data in transit, proxies must provide a trusted computing platform that prevents malicious software from taking control and compromising sensitive client and cloud application data.

V. CLIENT DATA PRIVACY

Often, clients must protect data privacy before sharing the data. Using encryption is not a viable option because maintaining the data's utility is a key requirement for many applications.

Privacy protection methods fall broadly 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?

Algorithms: Geometric Data Perturbation

Input: $X_{d \times N}$: the original dataset, w : weights of attributes in privacy evaluation, m : the number of iterations.

Output: R_t : the selected rotation matrix, the random translation, σ : the noise level,

P : privacy guarantee

Calculate the covariance matrix C of X ;

$p = 0$, and randomly generate the translation ;

For Each iteration do

Randomly generate a rotation matrix R ;

Swapping the rows of R to get R' , which maximizes $\min_{1 \leq i \leq d} \{1$

w_i

$(\text{Cov}(R'X - X)(i,i))$;

p_0 = the privacy guarantee of R' , $p_1 = 0$;

If $p_0 > p$ then

Generate \hat{X} with ICA;

$\{(1), (2), \dots, (d)\} = \text{argmin}\{(1),(2),\dots,(d)\} P_d$

$i=1 \text{ _PDF}(X_i, O(i))$

$p_1 = \min_{1 \leq k \leq d}$

1

W_k

$\text{Priv}(X_k, O(k))$

end if

if $p < \min(p_0, p_1)$ then

$p = \min(p_0, p_1)$, $R_t = R'$;

End if

End for

p_2 = the privacy guarantee to the distance-inference attack with the perturbation $G(X) = R_t X + \epsilon$.
Tune the noise level ϵ , so that $p_2 \leq p$ if $p < \epsilon$ or $p_2 > \epsilon$ if $p < \epsilon$.

Perturbation methods often produce data with high redundancies, which can lead to scalability issues in multi cloud environments; a client's request for data can result in a large communication overhead in the proxy network. Compression methods such as dictionary encoding can reduce both communication and query processing costs—for example, CSPs and proxies can perform much of the query processing over the encoded format.

Favorable solutions to ensure data privacy must employ flexible data perturbation methods that provide control over the tradeoff between the privacy guarantee and the utility of the query results. Perturbation methods must provide high accuracy for queries that involve a large number of records.

At the same time, they must introduce large amounts of noise in the results for queries over a few records, which is desirable for privacy. In the multiple-CSP context, a CSP can use local data perturbation techniques to perturb its sensitive data and then ship it to another CSP for collaborative query processing.

Local techniques permit query processing at one site to avoid on-the-fly data communication costs. When a query itself must be private, a CSP can limit query processing to its own site by using local techniques. In some applications, the receiving CSP need not perturb its own sensitive data. These situations present opportunities to further optimize the accuracy and efficiency of query processing that researchers can explore by judiciously determining which CSP should answer a particular query (when queries are not private and sharable). Finally, multi cloud scenarios require new privacy definitions that will allow formal proofs of privacy guarantees for protection schemes.

VI. CONCLUSION AND FUTURE ENHACEMENT

To facilitate dynamic collaboration between clouds, we proposed a framework that uses proxies to act as mediators between applications in multiple clouds that must share data. In 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 include refining the proxy deployment scenarios and development of infrastructural and operations components of a multicloud system.

VII. EXPERIMENTAL OUTCOMES

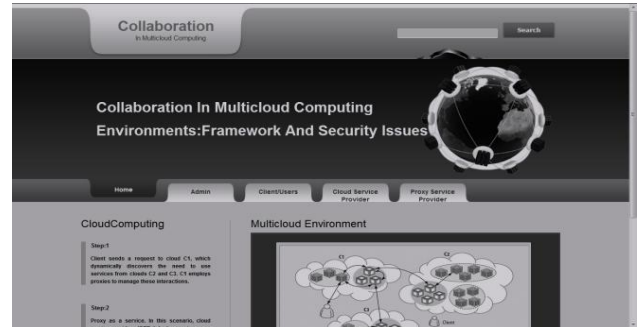


Fig. 5. Cloud Multicomputing



Fig. 6. Multi cloud Environment



Fig. 7. Uploading Page

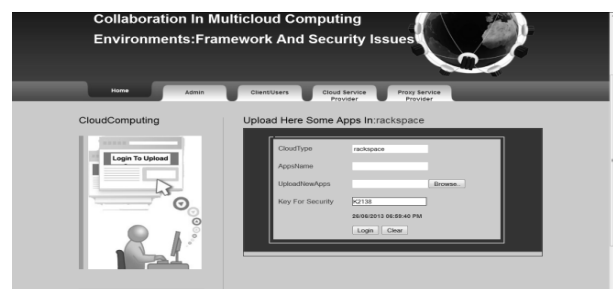


Fig. 8. Rackspace upload Page



Fig. 9. Cloud Service Provider



Fig.10. Client/User Register Page to Amazon

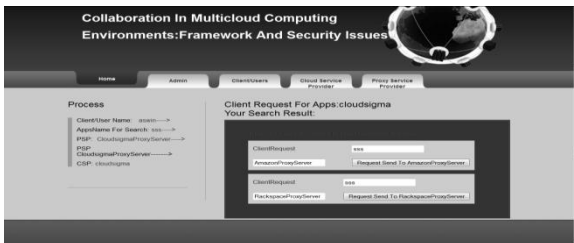


Fig. 11. Client Request for Applications



Fig. 12. Downloading page

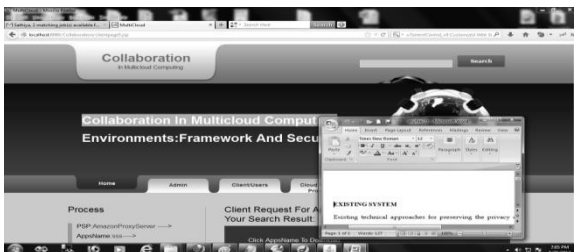


Fig. 13. Opening the Application.

REFERENCES

- [1] P.Mell and T.Grace, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory," Nat'l Inst. Standards and Technology,2008;http://csrc.nist.
- [2] D.Saravanan, Dr.S.Srinivasan, "Matrix Based Indexing Technique for Video Data ", International journal of Computer Science", 9 (5): 534-542, 2013,pp 534-542.
- [3] D.Saravanan, Dr.S.Srinivasan, " A proposed New Algorithm for Hierarchical Clustering suitable for Video Data mining.", International journal of Data Mining and Knowledge Engineering", Volume 3, Number 9, July2011.Pages 569-572
- [4] D.Saravanan, "Clustering the irregularity events in intelligence surrounding systems" Int. Journal of pure and applied mathematics, Vol. 119, No.12(2018), Pages 15025-15035, May-2018 (Special Issues) , ISSN:1311-8080.
- [5] D.N. Milne, I.H. Witten, and D.M. Nichols, "A Knowledge-Based Search Management (CIKM '07), pp. 445-454, 2007
- [6] D.Bernstein and D. Vij, "Intercloud Security Considerations," Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.
- [7] D.Saravanan, "Video data image retrieval using – BRICH", World journal of Engineering, Vol.14, Issuu 4, Pages 318-323, Aug 2017.
- [8] D.Saravanan, Dr.S.Srinivasan, "Video Image Retrieval Using Data Mining Techniques "Journal of Computer plications, Volume V, Issue No.1. Jan-Mar 2012. Pages39-42. ISSN: 0974-1925.
- [9] R.Navigli, P. Velardi, and A. Gangemi, "Ontology Learning and Its Application to Automated TerminologyTranslation," IEEE Intelligent Systems, vol. 18, no. 1, pp. 22-31, Jan./Feb. 2003.