Collaboration in Multicloud Computing Environments: Framework and Security Issues

Sanjana Sanap[*1], *Sawani Erande*[*2], *Ashish Thorat*[*3], *Shital Biradar*[*4], *Sarita Patil*[*5]

[*]*Department of Computer Engineering, G. H Raisoni College of Engineering and Management, Pune*

Abstract: Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Cloud mashups are a recent trend; mashups combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services. This service composition lets CSPs offer new functionalities to clients at lower development costs. Today, cloud mashups require pre-established agreements among providers as well as the use of custom-built, tools that combine services through low-level, tightly controlled and constraining integration techniques. This approach to building new collaborative services does not support agility, flexibility, and openness. Our proposed framework for generic cloud collaboration allows clients and cloud applications to simultaneously use services from cloud and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multi-cloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

I. INTRODUCTION

Cloud computing is an environment where the computing resources are outsource as a service through the internet. Clouds typically involve service providers, resource providers, and service users. The cloud computing model allows access to data and computer resources from anywhere that a network connection are available. The cloud computing service models are Software as a Service, Platform as a Service and Infrastructure as a Service. In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In Platform as a service, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. Cloud computing specification include network-based access channel, resource pooling, multitenancy, automatic and elastic provisioning and metering of resource usage. Clients can use these resources to host applications and even client can use to store their data. Rapid changes of resources demand can help to deal with variable demand and proving optimum resource utilization. As more organizations are using cloud computing, cloud service providers are developing new technologies to progress the cloud capabilities. Now the term, mashups are a new trend. It means combining services from multiple clouds into a single service or application. This service composition makes cloud service providers to propose new functionalities to clients at lower development costs.

Examples of cloud mashups and technologies are IBM's Mashups Center, Appirio Cloud Storage and Force.com for the Google App Engine. For example, cloudbased electronic medical record (EMR) management systems like Practice Fusion, Verizon Health Information Exchange, Medscribbler, and GE Healthcare Centricity Advance are emerging Cloud mashups want pre-established agreements among providers as well as the use of custom built, proprietary tools that combine services through low-level, tightly controlled and constraining integration techniques. This approach to building new collaborative services does not support stability, flexibility, and openness. Realizing multicloud collaboration's full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services reach across multiple clouds that lack pre-established agreements and proprietary collaboration tools. From a market perspective, it is doubtful that multiple CSP will agree on an easy and standardized way to access services, as this would give clients total freedom in changing providers, leading to increased open and direct competition with other providers. Cloud-based computing also introduces new security concerns that affect collaboration across multi cloud applications they are, increase in the attack surface due to system complexity, loss of client control over resources, threats that target exposed interfaces due to data storage in public domains, and data privacy concerns due to multitenancy. So there is need of developing multi cloud system which provides trust, security and safety for applications and data. Keeping all these drawbacks my focus is to develop cloud collaboration allows clients and cloud applications to simultaneously use services from multiple clouds.

There are restrictions in the current cloud computing model prevent direct collaboration among applications hosted by different clouds. A method that could remove these restrictions uses a network of proxies. A proxy is an

edge-node-hosted software instance that a user or CSP can delegate to carry out operations on its behalf. Proxies can act as mediators for collaboration among services on different clouds. As an example of proxy-facilitated collaboration between clouds, consider a case in which a user or CSP wishes to simultaneously use a collection of services from multiple clouds. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications. A user or CSP might employ multiple proxies to interact with multiple CSP.

Figure 1. Cloud Computing

The main objective of cloud computing is to support agility, flexibility and openness. Proprietary tools and services are integrated to control and monitor such a service. Different companies provide different services on cloud. Bringing these different services together and creating mashups require pre-established agreements among providers. Secure collaboration of such services is the need for tomorrow that motivated to take up this project.

II. LITERATURE SURVEY

1] *D. Bernstein and D. Vij, "Intercloud Security Considerations," Proc. 2nd Int'l Conf. Cloud Computing (CloudCom10), IEEE Press, 2010, pp. 537-544.*

The cloud computing design yields breakthroughs in geographical distribution, resource utilization efficiency, and infrastructure automation. These "public clouds" have been replicated by IT vendors for corporations to build "private clouds" of their own. Public and private clouds offer their end consumers a "pay as you go" model - a powerful shift for computing, towards a utility model like the electricity system, the telephone system, or more recently the Internet. However, unlike those utilities, clouds cannot yet federate and interoperate. Such federation is called the "Intercloud". Building the Intercloud is more than technical protocols. A blueprint for an Intercloud economy must be architected with a technically sound foundation and topology. As part of the overall Intercloud Topology, this paper builds on the technology foundation emerging for the Intercloud and specifically delves into details of Intercloud security considerations such as Trust Model, Identity and Access Management, governance considerations.

2] R. Buyya et al., "Market-Oriented Cloud Computing: Vision,Hype, and Reality of Delivering Computing as the 5th Utility,"Proc. 9th IEEE/ACM Int'l Symp. Cluster Computing andthe Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

This keynote paper: presents a 21st century vision of computing; identifies various computing paradigms promising to deliver the vision of computing utilities; defines Cloud computing and provides the architecture for creating market-oriented Clouds by leveraging technologies such as VMs; provides thoughts on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLAoriented resource allocation; presents some representative Cloud platforms especially those developed in industries along with our current work towards realizing market-oriented resource allocation of Clouds by leveraging the 3rd generation Aneka enterprise Grid technology; reveals our early thoughts on interconnecting Clouds for dynamically creating an atmospheric computing environment along with pointers to future community research; and concludes with the need for convergence of competing IT paradigms for delivering our 21st century vision.

3] B. Rochwerger et al., "Reservoir—When One Cloud Is Not Enough," Computer, Mar. 2011, pp. 44-51.

As cloud computing becomes more predominant, the problem of scalability has become critical for cloud computing providers. The cloud paradigm is attractive because it offers a dramatic reduction in capital and operation expenses for consumers. But as the demand for cloud services increases, the ensuing increases in cost and complexity for the cloud provider may become unbearable. We brie□y discuss the technologies we developed under the RESERVOIR European research project to help cloud providers deal with complexity and scalability issues. We also introduce the notion of a federated cloud that would consist of several cloud providers joined by mutual collaboration agreements

4] M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov./Dec 2011, pp.

Current cloud solutions are fraught with problems. They introduce a monolithic cloud stack that imposes vendor lock-in and don't let developers mix and match services freely from diverse cloud service tiers to configure them dynamically to address application needs. Cloud blueprinting is a novel approach that lets developers easily syndicate, configure, and deploy virtual service-based application payloads on virtual machine and resource pools in the cloud.

5] W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, special publication 800-144, Nat'l Inst. Standards and Technology

Cloud computing can and does mean different things to different people. The common characteristics most

interpretations share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

6] . N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," ACM Computing Surveys, Mar. 1989, pp.
This paper considers the problem of providing security to statistical databases against disclosure of confidential information. Security-control methods suggested in the literature are classified into four general approaches: conceptual, query restriction, data perturbation, and output perturbation. Criteria for evaluating the performance of the various security-control methods are identified.

7] L. Xiong, S. Chitti, and L. Liu, "Preserving Data Privacy in Outsourcing Data Aggregation Services," ACM Trans. Internet Technology, Aug. 2007, p. 17.
In this article, we describe two scenarios for outsourcing data aggregation services and present a set of decentralized peer-to-peer protocols for supporting data sharing across multiple private databases while minimizing the data disclosure among individual parties. Our basic protocols include a set of novel probabilistic computation mechanisms for important primitive data aggregation operations across multiple private databases such as max, min, and top k selection. We provide an analytical study of our basic protocols in terms of precision, efficiency, and privacy characteristics. Our advanced protocols implement an efficient algorithm for performing kNN classification across multiple private databases. We provide a set of experiments to evaluate the proposed protocols in terms of their correctness, efficiency, and privacy characteristics.

8] . D.J. Abadi, S. Madden, and M. Ferreira, "Integrating Compression and Execution in Column-Oriented DatabaseSystems," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD 06), ACM, 2006, pp. 671-682.
In this paper, we discuss how we extended C-Store (a column-oriented DBMS) with a compression sub-system. We show how compression schemes not traditionally used in roworiented DBMSs can be applied to column-oriented systems. We then evaluate a set of compression schemes and show that the best scheme depends not only on the properties of the data but also on the nature of the query workload.

III. LIMITATIONS OF EXISTING SYSTEM

The following restrictions in the Existing cloud computing model prevent direct collaboration among applications hosted by different clouds:

1] *Heterogeneity and tight coupling:* Clouds implement proprietary interfaces for accessing services, configuration, and Management, as well as interaction with other components of the cloud. Every service level of a cloud it integrates with lower service levels or is highly dependent on proprietary value added solutions that the cloud offers. This heterogeneity is interoperability between services of different clouds.

2] *Pre-established business agreements:* The current business model requires pre-established agreements between CSPs before collaboration can occur. These agreements are necessary for clouds to establish their willingness to collaborate and establish trust with one another. The lack of such agreements prohibits multicloud collaborative efforts due to incompatible intentions, business rules, and policies. Moreover, collaborations resulting from pre-established agreements typically exhibit tight integration between the participants and cannot be extended to provide universal and dynamic collaboration.

3] *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 interaction 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 a service delivery model limits a client's ability to customize a service and use it in combination with service offerings from different CSPs.

IV. MOTIVATION FOR CLOUD COLLABORATION

TECHNICAL MOTIVATION FOR CLOUD COLLABORATION TECHNOLOGY :

The top technical drivers for adopting a cloud collaboration strategy include the need for a single content repository, providing access to documents for mobile employees, and the requirement to securely share content with third-parties across the firewall. This growing need to share content across the firewall requires a secure and auditable platform that allows a business to retain control over a document throughout its lifecycle.

BUSINESS MOTIVATION FOR CLOUD COLLABORATION :

Organizations are searching for ways to work more closely with partners and customers and they are looking at cloud collaboration as a way to more closely connect with third-parties. Currently many organizations are only using email to share documents outside of their firewall. By implementing a cloud

collaboration strategy, organizations expect to have a centralized platform, where users cannot only exchange documents, but also share ideas and comments on existing work.

V. IMPLEMENTED SYSTEM

In this paper our implemented framework for generic 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 multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. And this approach work suitable strategies which are presented to reach the desired victim machine with a high probability, and show how to exploit this position for extracting confidential data, a cryptographic key, from the victim's VM. Finally it is proposed that, the usage of blinding techniques to fend Cross VM side-channel attacks. Proxies can be used for the purpose of collaboration of multiple clouds. 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: cloud service interaction on behalf of a client, data processing using a rich set of operations, caching of intermediate results, and routing, among others. With these additional functionalities, proxies can act as mediators for collaboration among services on different clouds.
Such systems can use several possible strategies for placing proxies in the proxy network.

- Cloud-hosted proxy
- Proxy as a service
- Peer-to-peer proxy
- On-premise proxy
- Hybrid proxy infrastructure

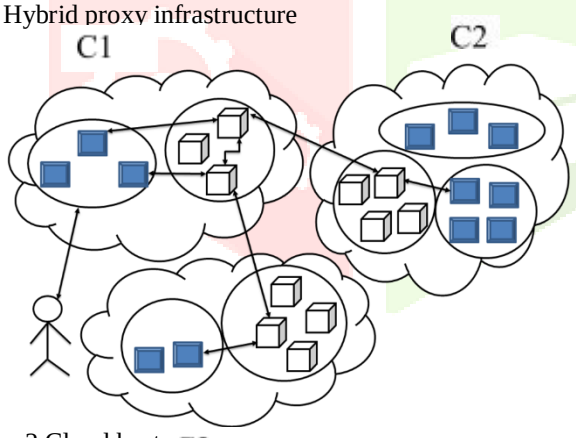

Figure 2 Cloud host

In our implemented system we are placing proxy within cloud infrastructure and manages all the proxy with administrative domain. All the service request from client that wish to collaborate are manage under administrative domain. The proxy instances are CSP specific as shown in Figure 2.In our system client send request to cloud c1, which identify that need to use services from c2 and c3. C1 use proxy to do further interactions. It provide more security among all architecture because all interaction done inside administrative domain.

In our implemented architecture user send request to C1 if data is not available on C1 then proxy present in C1 send request to other cloud on behalf of user and search for data on other cloud which are collaborating with C1 like C2 and C3 as shown in Figure2 . In this way data is make available to user from different cloud using proxy framework. Proxy framework are working on behalf of user for another cloud. If data is found on another cloud then data is send to respective user.

ADVANTAGES OF IMPLEMENTED SYSTEM:

- Implemented networks of proxies to overcome existing restrictions.
- Proxy is an edge-node-hosted software instance.
- Proxies can facilitate collaboration without requiring prior agreements between the cloud service providers.

VI. ALGORITHM

UPLOADING ALGORITHM:

Step1: validate login from CSP by providing valid user id and password
If validation succeeds
{
Show the new page to upload data and go to step2
}
else
{
Go to step 3;
}

Step 2: If validation succeeds
{
Select the document need to be uploading. Select the cloud and click the upload button.
}
else
{
Give error message if uploading failed
}

Step 3: Ask for valid user name and password.

END

DOWNLOADING ALGORITHM:

Step 1: client login with appropriate cloud type valid user id and password
If validation succeeds

{
Go to step 2 or (Client requesting for data page visible to user)
}
else
{
Go to step 3.
}
Step 2: Send a request of file to the CSP
If file available with current CSP
{
Send download link to user
}
else
{
Send request to another CSP via Proxy Server CSP and check for the request made by CSB Repeat step 2 until we check all CSP for request
}

Step 3: Ask for valid user name and password.

End

ENCRYPTION ALGORITHM:

Step 1: Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

Step 2: XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

Step 3: Encrypt the string with the Blowfish algorithm, using the data file described in steps (1) and (2).

Step 4: Replace P1 and P2 with the output of step (3).

1. Encrypt the output of step (3) using the Blowfish algorithm with the modified data
2. Replace P3 and P4 with the output of step (5).

Figure 3 Activity Digram

VII. IMPLEMENTATION PHASE

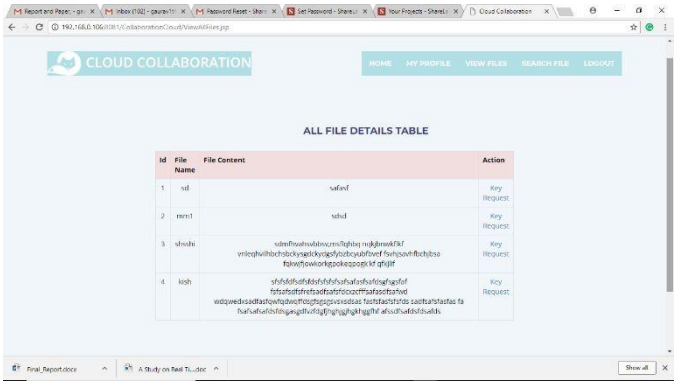

Figure 4. View Files

As shown in figure 4 we can see all the contain of file and send key request to admin if want to download that file

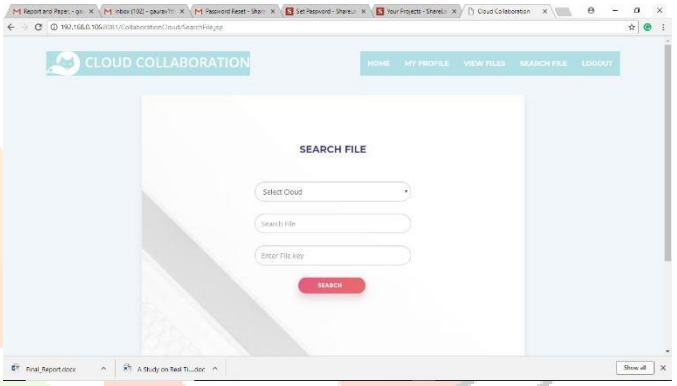

Figure 5. View Files

As shown in figure 5 we can search file on cloud if file not present on our csp we can send request to another csp by selecting another csp name in Select cloud option.

Figure 6. View Files

If file present on out csp then we can download that file by entering key which we receive on our mail.

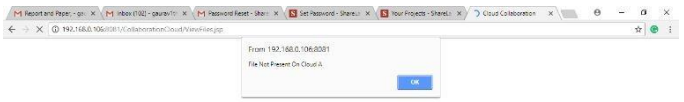

Figure 7. View Files

If file not present on csp we can search that file on another csp By using our proxy and can download that file.

IX. CONCLUSION

In this proposed framework and uses the proxy for collaboation. Here, proxies act as mediators between multiple cloud applications who want to collaborate to share data. The proposed framework has the potential to overcome many constraints in the current cloud computing model that could prevent dynamic collaboration between applications hosted by different cloud systems. Future research guidelines for the proposed project include the perfection of proxy deployment scenarios and the development of the infrastructure and operating components of a multicloud system.

Future work for the proposed framework includes the refinement of proxy deployment scenarios and the development of infrastructural and operational components of a multicloud system. This should be accompanied by the implementation of an experimental platform using open source tools and libraries that work in combination with real-world cloud services to evaluate system functionality and limitations and refine and explore techniques that can identify proxies automatically based on the application

REFERENCES

[1]. 2. D. Bernstein and D. Vij, "Intercloud Security Considerations,"*Proc. 2nd Int'l Conf. Cloud Computing* (CloudCom10), IEEE Press, 2010, pp. 537-544.

[2]. R. Buyya et al., "Market-Oriented Cloud Computing: Vision,Hype, and Reality of Delivering Computing as the 5th Utility,"*Proc. 9th IEEE/ACM Int'l Symp. Cluster*

[3]. B. Rochwerger et al., "Reservoir—When One Cloud Is Not Enough," *Computer*, Mar. 2011, pp. 44-51.

[4]. M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," *IEEE Internet Computing*, Nov./Dec 2011, pp. 74-79.

[5]. 8. W. Jansen and T. Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, special publication 800-144,Nat'l Inst. Standards and Technology, 2011, p. x + 70

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

[7]. 16. L. Xiong, S. Chitti, and L. Liu, "Preserving Data Privacy in Outsourcing Data Aggregation Services," *ACM Trans. Internet Technology*, Aug. 2007, p. 17.

[8]. 17. D.J. Abadi, S. Madden, and M. Ferreira, "Integrating Compression and Execution in Column-Oriented DatabaseSystems," *Proc. ACM SIGMOD Int'l Conf. Management of Data* (SIGMOD 06), ACM, 2006, pp. 671-682.