An Approach For Scheme And Surveillance Concerns in Alliance Of Multi Cloud Habitat

[1]Pokala Chandana, [2]Arif Mohammad Abdul
Dept of CSE
GITAM University , Hyderabad

Abstract-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. The recent surge in 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 (or clients). They include applications delivered as services, as well as the hardware and software systems providing these services. Cloud computing characteristics include a ubiquitous (network-based) access channel; resource pooling; multi tenancy; automatic and elastic provisioning and release of computing capabilities; and metering of resource usage (typically on a pay-per-use basis). Virtualization of resources such as processors, network, memory, and storage ensures scalability and high availability of computing capabilities. 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. Rapid provisioning and dynamic reconfiguration of resources help cope with variable demand and ensure optimum resource utilization.

General Terms:
Optimization, Elasticity, Multi-Tenancy

Keywords
Virtual Machines, Storage, Optimization

I. INTRODUCTION

Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization generalizes the physical infrastructure, which is the most rigid component, and makes it available as a soft component that is easy to use and manage. By doing so, virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. On the other hand, autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process and reduces the possibility of human errors. Users face difficult business problems every day. Cloud computing adopts concepts from Service-oriented Architecture that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way. Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loop in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

II. BACKGROUND ISSUES

Threats and opportunities of the cloud:

Critical voices including GNU project initiator Richard Stallman and Oracle founder Larry Ellison warned that the whole concept is rife with privacy and ownership concerns and constitute merely a fad. However, cloud computing continues to gain steam with 56% of the major European technology decision-makers estimate that the cloud is a priority in 2013 and 2014, and the cloud budget may reach 30% of the overall IT budget.

According to the Tech Insights Report 2013: Cloud Succeeds based on a survey, the cloud implementations generally meets or exceeds expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Several deterrents to the widespread adoption of cloud computing remain. Among them, are: reliability, availability of services and data, security, complexity, costs, regulations and legal issues, performance, migration, reversion, the lack of standards, limited customization and issues of privacy. The cloud offers many strong points: infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. The early 2010s cloud market is dominated by software and services in SaaS mode and IaaS (infrastructure), especially the private cloud. PaaS and the public cloud are further back.

Privacy:

The increased use of cloud computing services such as Gmail and Google Docs has pressed the issue of privacy concerns of cloud computing services to the utmost importance. The provider of such services lie in a position such that with the greater use of cloud computing services has given access to a plethora of data. This access has the immense risk of data being disclosed either accidentally or deliberately. Privacy advocates have criticized the cloud model for giving hosting companies' greater ease to control—and thus, to monitor at will—communication between host company and end user, and access user data (with or without permission). Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million telephone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity. A cloud service provider (CSP) can complicate data privacy because of the extent of virtualization (virtual machines) and cloud storage used to implement cloud service. CSP operations, customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud; this can lead to legal concerns over jurisdiction. While there have been efforts (such as US-EU Safe Harbor) to "harmonies" the legal environment, providers such as Amazon still cater to major markets (typically to the United States and the European Union) by deploying local infrastructure and allowing customers to select "availability zones." Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. This becomes a major concern as these service providers, who employ administrators which can leave room for potential unwanted disclosure of information on the cloud.

Privacy solutions:

Solutions to privacy in cloud computing include policy and legislation as well as end users' choices for how data is stored. The cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used. Cloud service users can encrypt data that is processed or stored within the cloud to prevent unauthorized access

Security:

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. The relative security of cloud computing services is a contentious issue that may be delaying its adoption. Physical control of the Private Cloud equipment is more secure than having the equipment off site and under someone else's control. Physical control and the ability to visually inspect data links and access ports is required in order to ensure data links are not compromised. Issues barring the adoption of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services. This delivers great incentive to cloud computing service providers to prioritize building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support and legal support.

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

III. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

In the previous section, we have discussed generic set of security concerns observed in public and hybrid clouds. We now turn our focus to some atypical cloud specific security issues. In particular, cloud does bring out a set of unique challenges like:

Abstraction: Cloud provides an abstract set of service end-points. For a user, it is impossible to pin-point in which physical machine, storage partition (LUN), network port MAC address, switches etc. are actually involved. Thus, in event of security breach, it becomes difficult for a user to isolate a particular physical resource that has a threat or has been compromised.

***Lack of execution controls*: **The external cloud user does not have fine-gained control over remote execution environment. Hence the critical issues like memory management, I/O calls, access to external shared utilities and data are outside the purview of the user. Client would want to inspect the execution traces to ensure that illegal operations are not performed.

***Third-party control of data*: **In cloud, the storage infrastructure, and therefore, the data possession is also with the provider. So even if the cloud provider vouches for data integrity and confidentiality, the client may require verifiable proofs for the same.

***Multi-party processing*: **In multi-cloud scenario, one party may use part of the data which other party provides. In absence of strong encryption (as data is being processed), it becomes necessary for participating cloud computing parties to preserve privacy of respective data.

Data breach is a big concern in cloud computing. A compromised server could significantly harm the users as well as cloud providers. A variety of information could be stolen. These include credit card and social security numbers, addresses, and personal messages. The U.S. now requires cloud providers to notify customers of breaches. Once notified, customers now have to worry about identify theft and fraud. While providers, have to deal with federal investigations, lawsuits, and bad reputation. Customer lawsuits and settlements have resulted in over $1 billion in losses to cloud providers. Cloud collaboration brings together new advances in cloud computing and collaboration that are becoming more and more necessary in firms operating in an increasingly globalised world. Cloud computing is a marketing term for technologies that provide software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. A parallel to this concept can be drawn with the electricity grid, where end-users consume power without needing to understand the component devices or infrastructure required to provide the service. Collaboration, in this case, refers to the ability of workers in a company to work together simultaneously on a particular task. In the past, most document collaboration would have to be completed face to face. However, collaboration has become more complex, with the need to work with people all over the world in real time on a variety of different types of documents, using different devices. While growth in the collaboration sector is still growing rapidly, it has been noted that the uptake of cloud collaboration services has reached a point where it is less to do with the ability of current technology, and more to do with the reluctance of workers to collaborate in this way. A report by Erica Rugullies mapped out five reasons why workers are reluctant to collaborate more. These are: People resist sharing their knowledge. Users are most comfortable using e-mail as their primary electronic collaboration tool. People do not have incentive to change their behavior. Teams that want to or are selected to use the software do not have strong team leaders who push for more collaboration. Senior management is not actively involved in or does not support the team collaboration initiative.

As a result, many providers of cloud collaboration tools have created solutions to these problems. These include the integration of email alerts into collaboration software and the ability to see who is viewing the document at any time. All the tools a team could need are put into one piece of software so workers no longer have to rely on email based solutions. Recently, cloud collaboration has seen rapid evolution. In the past, cloud collaboration tools have been quite basic with very limited features. Newer packages are now much more document-centric in their approach to collaboration. More sophisticated tools allow users to "tag" specific areas of a document for comments which are delivered real time to those viewing the document. In some cases, the collaboration software can even be integrated into Microsoft Office, or allow users to set up video conferences. Furthermore, the trend now is for firms to employ a single software tool to solve all their collaboration needs, rather than having to rely on multiple different techniques. Single cloud collaboration providers are now replacing a complicated tangle of instant messengers, email and FTP. Cloud collaboration today is promoted as a tool for collaboration internally between different departments within a firm, but also externally as a means for sharing documents with end-clients as receiving feedback. This makes cloud computing a very versatile tool for firms with many different applications in a business environment.

The best cloud collaboration tools:

Use real-time commenting and messaging features to enhance speed of project delivery

Leverage presence indicators to identify when others are active on documents owned by another person.

Allow users to set permissions and manage other users' activity profiles.

Allow users to set personal activity feeds and email alert profiles to keep abreast of latest activities per file or user.

Allow users to collaborate and share files with users outside the company firewall.

IV. ASSESSMENT FRAMEWORK

Comply with company security and compliance framework Ensure full audit ability of files and documents shared within and outside the organization Reduce workarounds for sharing and collaboration on large files. A 2011 report by Gartner outlines a five stage model on the maturity of firms when it comes to the uptake of cloud collaboration tools. A firm in the first stage is said to be "reactive", with only email as a collaboration platform and a culture which resists information sharing. A firm in the fifth stage is called "pervasive", and has universal access to a rich collaboration toolset and a strong collaborative culture. The article argues that most firms are in the second stage, but as cloud collaboration becomes more important, most analysts expect to see the majority of firms moving up in the model.

Mashups:

Information-integration, Presentation-layer *Mashups:* Is the next wave of mashups rising? Since Paul Rademacher’s early experiments with housingmaps.com back in 2005, Google Maps mashups have become ubiquitous. The Google Maps API is popular because it enables developers to build Web applications that output information in a more user-friendly representation, such as real estate locations or crime scenes. Yahoo has developed some really cool tools that further reduce the learning curve of processing, mixing and restructuring information and media from different sources into a single representation. However, it seems like these are mashups of the old days. A new dawn is breaking… Platform Mashups The new type of mashup that we can see today combines Cloud Computing services and integrates them into a single service or application. Amazon's Grep The Web is a good example for Cloud Computing service compositions within the domain of a single provider. However, the recent announcement of Appirio's Refer My Friends App shows that also cross-Cloud mashups are viable. Other examples for cross-Cloud mashups are Facebook + EC2 back-end and Force.com + AppEngine back-end (although it is probably only a matter of time until will become one of the single-domain examples). What are the main motives to combine Cloud Computing services? One motive is similar to the old Google Maps-style mashups: integrate information from different domains. The other motive: make your service scalable by extending it with a Cloud back-end. Still, there are more interesting mashup opportunities at the horizon… A mashup is a Web page or application that uses and combines data, presentation or functionality from two or more sources to create new services. The term implies easy, fast integration, frequently using open APIs and data sources to produce enriched results that were not necessarily the original reason for producing the raw source data. The main characteristics of the mashup are combination, visualization, and aggregation. It is important to make existing data more useful, moreover for personal and professional use. To be able to permanently access the data of other services, mashups are generally client applications or hosted online. In the past years, more and more Web applications have published APIs that enable software developers to easily integrate data and functions instead of building them by themselves. Mashup composition tools are usually simple enough to be used by end-users. They generally do not require programming skills and rather support visual wiring of GUI widgets, services and components together.

A consumer mashup is an application that combines data from multiple public sources within a browser and organizes it through a simple browser user interface. An enterprise mashup , also often called a business mashup, is an application that combines data from multiple internal and public sources, and publishes the results to enterprise portals, application development tools, or as a service in a service-oriented architecture. A data mashup, opposite to the consumer mashups, combine similar types of media and information from multiple sources into a single representation. The combination of all these resources create a new and distinct Web service that was not originally provided by either source. (DaaS – Data as a Service)

Why Mashup?

Access both internal and external information faster

Mashups access – and combine – data faster than almost any other method, avoiding complex APIs and middleware and leveraging information that is easy to access. For certain business scenarios, where speed is critical, mashups are a fast way to get to critical business information. Make better business decisions Mashups give business users the ability to assemble their own 'situational applications' in response to ever-changing business requirements. Combine your business data in new ways Mashups integrate different data sources – corporate data from current systems mashed up with external data, all provided to the user in a browser for efficiency and speed.

V.AUTHENTICATION AND IDENTITY MANAGEMENT

Users can easily access their personal information using cloud services and the authentication and identity management module is also available for various services across the Internet. The Identity management (IDM) mechanism is used to authenticate users and services A potential problem area with IDM in the cloud concerns the interoperability issues that may result from the use of different identity tokens and different identity negotiation protocols. An IDM system should be able to accommodate privacy concerns for the protection of private and sensitive information associated with users and processes. In relation to interoperability problem mentioned above, user-centricity is an essential characteristic for providing flexible, scalable IDM service. User-centric IDM has recently received significant attention for handling private and critical identity attributes . In this approach, an identity has identifiers or attributes that identify and define each user. The user centric approach allows users to control their own digital identities and also takes away the complexity of IDM from the enterprises, allowing users to focus on their own functions. Based on the approaches given, it is desirable to have a functional scheme to handle the authentication process and manage IDM

VI. CONCLUSION

The recent surge in 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 (or clients). They include applications delivered as services, as well as the hardware and software systems providing these services. Cloud computing characteristics include a ubiquitous (network-based) access channel; resource pooling; multi tenancy; automatic and elastic provisioning and release of computing capabilities; and metering of resource usage (typically on a pay-per-use basis). Although there are many advantages to using a cloud-based system, practical problems remain that have to be solved before the technology can be more fully deployed, particularly those problems related to service level agreements, security, privacy, and power efficiency. the proposed framework include refining the proxy deployment scenarios and development of infrastructural and operational components of a multi cloud system.

REFERENCES

[1] Amazon Elastic Compute Cloud web services at *http://aws.amazon.com/ec2*

[2] SalesForce Force.com Platform as a service at *http://developer.force.com*

[3] NetSuite SaaS portal at *http://www.netsuite.com*

[4] Gartner DataQuest Forecast on Public Cloud Services DocID G00200833, June 2, 2010

[5] Chow,R.,Gotlle,P.,Jakobsson, E.S.,Staddon,J., Masuoka,R., and Molina,J.;2009, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009

[6] Gellman, R., Privacy in the Cloud: Risks to Privacy and Confidentiality in Cloud Computing. *Technical Report prepared for World Privacy Forum*, 2009.

[7] Mohamed Almorsy, John Grundy, and Amani S. Ibrahim, "TOSSMA: A Tenant-Oriented SaaS Security Management Architecture", 5th IEEE Conference on Cloud computing IEEE, 2012.

[8] Yashaswi Singh, Farah Kandah, Weiyi Zhang, "A Secured Cost-effective Multi-Cloud Storage in Cloud Computing", IEEE INFOCOM Workshop on Cloud Computing, 2011.

[9] Anton Beloglazov, Jemal Abawajy, Rajkumar Buyyaa, "Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing", Future Generation Computer Systems ELSEVIER , pp. 755–768, 2011.

[10] Jose Luis Lucas-Simarro, Rafael Moreno-Vozmediano, Ruben S. Montero and Ignacio M. Llorent, "Cost optimization of virtual infrastructures in dynamic multi-cloud scenarios", Concurrency and Computation: practice and experience Concurrency Computat.: Pract. Exper. Published online in Wiley Online Library (wileyonlinelibrary.com). 2012.

AUTHOR'S PROFILE:

1. **Ms.Pokala Chandana** student in GITAM University, Hyderabad pursuing her M-Tech in dept of CST, received Bachelor of Engineering(B.E) in computer science in 2008 from Swami Vivekananda Institute Of Technology and research area in the field of cloud computing.

2. **Mr.Arif Mohammad Abdul** working as an assistant prof. in Dept.of CSE, GITAM university, Hyderabad.He received his M-Tech degree in the 2010 from Sri Indu College Of Engineering & Technology, Hyderabad and received Bachelor of Engineering (B.E) in computer science in 2004 from Maharshi Dayanand University Haryana. Registered PhD in the computer Science in the year 2012 and he is doing research in the area of Trusted Cloud Computing. His Research papers are "Trusted System in Cloud Environment" in the area of Cloud Computing in the year 2013 and "A Novel Approach For Extracting Medical Reports Using Mining Techniques" in the area of Data Mining in the year 2010.