Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Architecture of Multicloud

Tanvi Sharma
Department CSE &(A.I.T.M)MDU
India

Dr.Deepti Sharma
Head Of Department CSE &(A.I.T.M)MDU
India

Abstract— Cloud computing is an innovation of existing technology which provides long-dreamed vision of Computing as utility. The emergence of this novel technology in IT business has decoyed most of organizations in both private and public sector. With this new advent Cloud services can be availed without any capital investment such as any infrastructure as they are commoditized. Cloud users get services in pay per use fashion this means user need to pay only for the resources which he used or utilized and enjoy many benefits of cloud including low cost and accessibility from around the world. However But truly said everything has its pros and Cons. Point comes what are the Cons of such a beneficial technology that has exploded market with great capabilities and seems ever promising. Cloud Computing has motivated industries, academia, businesses to adopt cloud computing to host high computationally intensive application down to light weight application and services. As everything comes with certain Cons in Cloud computing also there is tradeoff between security and high computability still there are a lot of open issues that impact the cloud computing model credibility and pervasiveness.Users have various security concerns because user shows a great trust towards service provided with their important data and resources. With a single cloud service provider there might be the chance or risk of service not available when it is most required, failure of single cloud possibility and insider theft of data. Moving towards multiple clouds can address security problems

Keywords— Cloud, Security, Single Cloud, Multi Cloud, Fragmentation

I. INTRODUCTION

Cloud computing is a phrase used to describe a variety of concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

II. MOVING TOWARDS MULTI CLOUD

The very first question that arises when once hears about Multi Cloud. What is multi cloud?
Multi-cloud strategy is the concomitant use of two or more cloud services to minimize the risk of widespread data loss or downtime due to a localized component failure in a cloud computing environment.
The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of no collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data applications of a specific cloud user.
The idea of making use of multiple clouds has been proposed by Bernstein and Celesti there previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios.

III. Prior Work

Cloud computing offers scalable resources as provisioned over internet but it also creates a large number of security issues and challenges. As stated in Paper Cloud Computing - Concepts, Architecture and Challenges By Yashpalsinh Jadeja and Kirit Modi this Paper tells us in detail about what actually Cloud computing is. How it emerged as a powerful trend in IT, that moves computing and data away from desktop and portable PCs into large data centers.But as we all

know that every good thing come with some issues that also need to be dealt with ,we analyzed and understood all this with the help from paper An Analyses of cloud computing security issues by Akhil Behl and Kanika Behl it tell in great detail about various security concerns in Cloud computing that are to be dealt with in order to make full efficient use of this advancement and remove that threats. Cloud as mentioned earlier give services in three broad categories as SaaS,PaaS and IaaS where SaaS is a phenomenon where the a capability is provided to user or customer as the provider's application running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).On the other side PaaS is called as Platform as a service it allow to consumer to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. Whereas IaaS is Infrastructure as a Service it provide to the consumer to provision processing, storage, networks, and other fundamental Computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS. With these three capabilities there lie some problems such as Multi-tenancy which means various consumer's resources reside on single Cloud this is called Multitenancy then there is Elasticity which a phenomenon in cloud computing that give power to user to scale up or down resources as and when required.

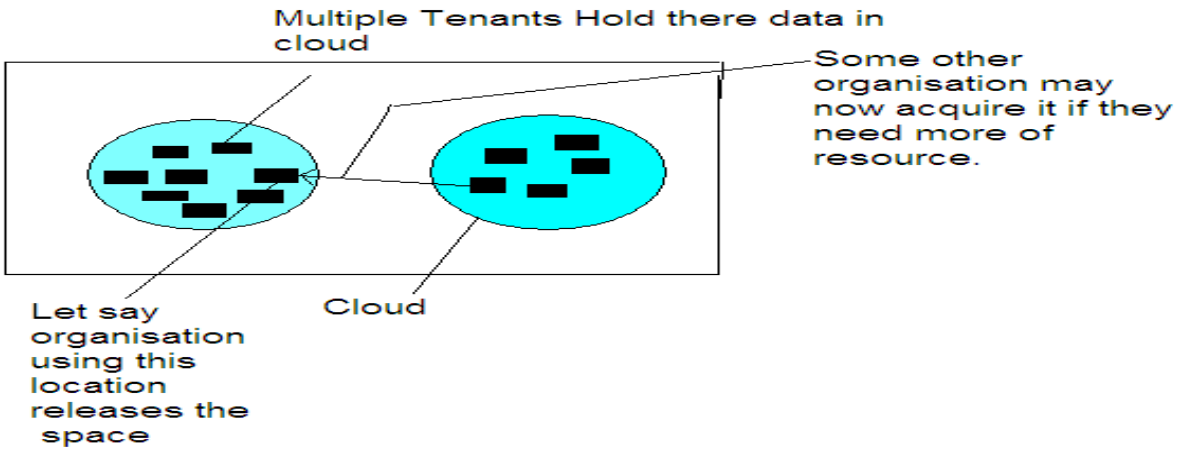


Diagram shows Problem of Confidentiality leakage in a Multitenant Cloud environment. Data is the Life of IT world so its security but this becomes a great challenge when we talk about cloud. Trusting a third party to keep our data safe takes a lot of guts keeping a full trust on third party the cloud provider all the threats associated with data in clouds are well stated in Security Framework of Cloud Data Storage Based on Multi Agent System- By Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah & Masrah Azrifah Azmi Murad. This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid a UN trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed cloud servers or CDS. It is a must when employing a public cloud due to public clouds accessibility nature. Asserting confidentiality of cloud users' profiles and protecting their data, that is virtually accessed, allows for cloud data security protocols to be enforced at various different layers of cloud applications. Goal of correctness assurance to ensure cloud users that their cloud data are indeed stored appropriately and kept intact all the time in the cloud to improve and maintain the same level of storage correctness assurance even if cloud users modify, delete or append their cloud data files in the cloud. Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among cloud vendors as well as in the delivery models .

Now to remove the threats that we discussed in Cloud computing Multitenant environment there is a secure way.secure as compared to Basic Cloud Computing discussed Earlier. This all can be more clear with the help of Cloud Computing Security: From Single to Multi-Clouds by Mohammed A. AlZain, Eric Pardede, Ben Soh and James A. Thom This paper focuses and throw some light on the various problem associated with single Clouds and what happened that motivated the cloud providers to move to this new Idea called as Multi Cloud.

Single Cloud doesn't mean that we have only one cloud but it has a different approach as when the cloud were new in the market cloud provider use to allocate one big cloud dedi catedly to a consumer, all its resources or the services are provided by single cloud. As the time moved on it was noticed that in this way all the security risks that we discussed

above are more likely to occur. To resolve this problem a new approach is used to use Multi clouds with the word multi cloud we mean that the data or services that were earlier stored or utilized through single cloud is now distributed to multiple cloud. With this new approach risk involved with single cloud are reduced tremendously as data is wide spread if it is not available from one location other cloud has some this to give all the data, services etc are not widespread. Responsibility of data security doesn't end here it doesn't mean as we deployed the multicloud environment our data is now safe from all the threats we discussed earlier. Security is still a concern and we should move in direction to make cloud more and more efficient and secure this can be more cleared through paper Security and Privacy-Enhancing Multi cloud Architectures Architecture-By Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau.The basic idea given by this paper is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non collaborating cloud service providers in order to provide better architecture to enhance security in a multi cloud.

IV. SECURITY RISKS OF CLOUD COMPUTING

At the core of the legal concern over cloud computing is data. In the digital world, data is constantly being created, archived, shared--and even occasionally destroyed. The default position of the internet is open, meaning all the data that interacts with the internet can be shared. This, of course, presents a challenge for school personnel who are under legal obligation to keep the information secure.[18]

There seems to be no area of Information and Communication Technology that is not affected by Cloud Computing. Two main issues exist with security and privacy aspects of Cloud Computing:

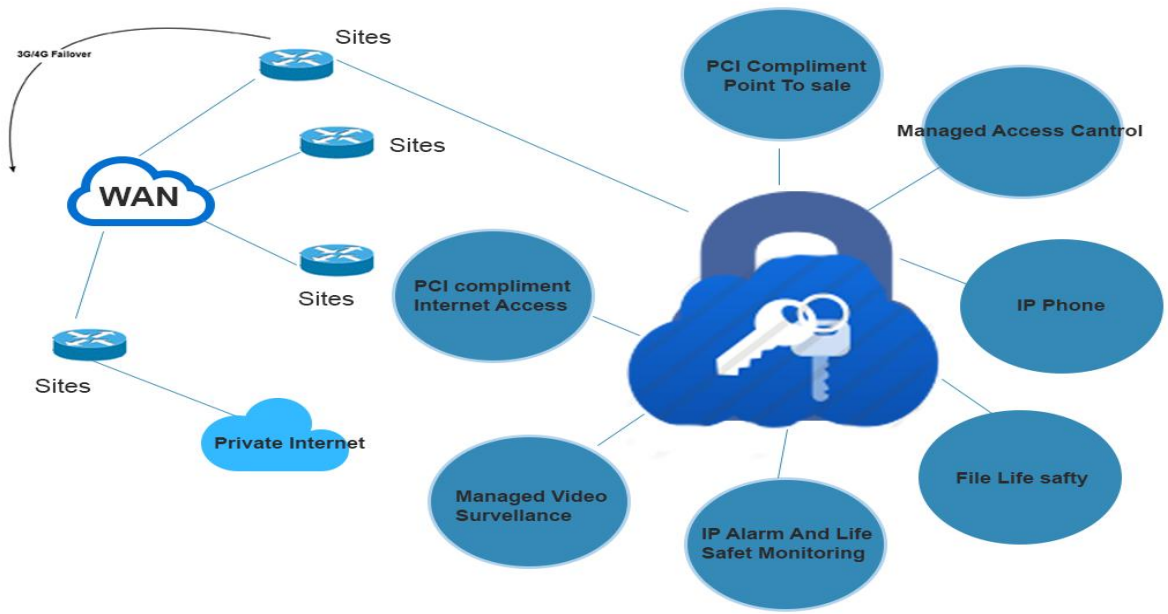
1. loss of control over data-As data and Information will be shared with a third party cloud computing user want to avoid untrusted cloud providers. Protecting private and important information such as credit card details or a patient's medical record from attackers or malicious insiders is of critical information.

The organizations have data as the most critical asset for an organization and to trust the outsider that he will keep our assets safe and well confidential is very important. There could be a chance that data could be unavailable when required the most reason behind such failure could be some miss happening that resulted into non availability of data when its need was critical. These issues should be taken care of well in advance at the time of SLA (Service level agreement) as what should be the backup plan when such thing happens.

As from the organization's end there is loss of control over the Organization's data and it now becomes the responsibility of the service provider how he manage it. A very critical form of data or information is just like a normal piece of data for the service provider the control over the data or its safety should always be ensured by the third party or the cloud provider.

2. Dependence on the Cloud Computing provider-As discussed on the above point that there is loss of control from the organization's side then the responsibility of data lies on Cloud computing provider. He may never understand the criticality of certain data from the bulk of other data from the same organization. Organizations own data availability and security depends on the cloud Provider. A great responsibility lies on the shoulder of the cloud provider to make data safe and to make it available as and when required. These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.

Security Model for multi Cloud

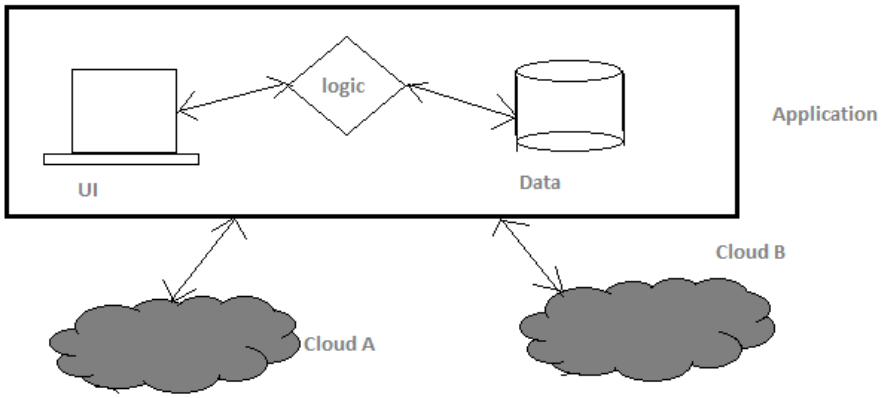


V. PROPOSED RESEARCH

The idea of making use of multiple clouds has been proposed by Bernstein and Celesti however, this previous work did not focus on security. Since then other approaches considering the security effect have been proposed, these approaches are operating on different cloud surveys levels, are partly combined with cryptographic methods and targeting different usage scenarios. Through various papers we analyzed various models of different architectural patterns for distributing resources to multiple cloud providers. The model that we are following contains four architectural patterns.

Replication of Application, Partition of application System into tier, Partition of Application Logic into Fragments and Partition of application data into Fragments. These are the kind of four approaches through which we can fragment the organization's assets into multiple clouds to keep it safe and secure.

The following diagram display the replication of Application which allows the organization to receive multiple results from one operation performed in distinct clouds and compare them with in own premise. This enable user to get an evidence of integrity and of the result. But the others approaches still need to be evaluated.



Each of the architectural patterns provides individuals security merits which map to different application scenario needs. We can also think about combining these four architecture that might result in combined security merits but also in higher deployment and runtime effort. In future work I will evaluate and analyze other architecture in order to provide and enhance security in multi clouds .

VI. Conclusion

with these following examples we came to know that Cloud computing is not fully mature and still lot needs to be explored. After our current work we are claiming that security is the most important threat to both the users and the vendors of cloud computing. Vendors, Researchers, and IT security professionals are working on security issues associated with cloud computing. Different models and tools have been proposed but still nothing fruitful found. While doing research on security issues of cloud computing we came to know that there are no security standards available for secure cloud computing. In our future work we will work on security standards for secure Computing on Multi clouds.

ACKNOWLEDGMENT

I would like to place on record my deep sense of gratitude to **Dr. Deepti Sharma** Head of department of Computer Science and Engineering, A.I.T.M,Palwal, India for her generous guidance, help and useful suggestions. I express my sincere gratitude to **Mr.P.S Bishnoi** Principal of A.C.T.M Palwal India, for his stimulating guidance, continuous encouragement and supervision throughout the course of present work.

I also wish to extend my thanks to **Mr. Mahesh Singh** senior asst professor A.I.T.M for attending my seminars and for their insightful comments and constructive suggestions to improve the quality of this research work.I am extremely thankful to **Dr. R.S.Chaudhary** Director A.E.I Palwal, for providing Me infrastructural facilities to work in, without which this work would not have been Possible.

Tanvi Sharma

REFERENCES

[1] Cloud Computing Architectures Based Multi Tenant IDS Elmahdi Khalil , Saad Enniari and Mo tapha ZbakhAuthors.
[2] Cloud security issues Balachandra reddy kandukari,Ramakrishna Paturi V and Dr. Atanu Rakshit
[3] Security architecture for cloud computing Platform Sanjaya Dahal
[4] Overlay Architectures enabling Cloud Computing for Multi-Level Security Environments Christopher C. Lamb and Gregory L. Heileman
[5] A Comparison of Secure Multi-tenancy Architectures for File system Storage Clouds.Anil Kurmus1, Moitrayee Gupta?2, Roman Pletka1, Christian Cachin1, and Robert Haas1
[6] Security and Privacy-Enhancing Multicloud Architectures Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE,Luigi Lo Iacono, and Ninja Marnau

[7] Notorious 9 top security threats in 2013
[8] Multi-Cloud Architecture to Reduce Security Risks in Cloud Computing Vinod Kumar Paidi* , P.Varaprasada Rao
[9] http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg
[10] http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx
[11] D. Talbot. Security in the Ether. Technology Review, pages 36–42
[12] Hassan Takabi and James B.D.Joshi,Security and Privacy Challenges in Cloud Computing Environments, University of Pittsburgh, Gail-Joon Ahn,Arizona State University.
[13] C. Cachin and S. Tessaro, "Optimal resilience forerasure-coded Byzantine distributed storage",DISC:Proc. 19thIntl.Conf. on DistributedComputing, 2005, pp. 497-498.[14] M. Castro and B. Liskov, "Practical Byzantine faulttolerance", Operating Systems Review
[14] http://thejournal.com/articles/2013/10/01/the-major-cloud-computing-problems-youre-not-paying-attention-to.aspx#TMZX9ZADRdseyyWV.99
[15] http://www.cepis.org/index.jsp?p=641&n=825&a=4758#sthash.7AZ6fRvt.dpuf
[16] http://en.wikipedia.org/wiki/Cloud_computing]
[17] A Brief History of Cloud Computing by JamesSteddum in Cloud, Technology
[18] Cloud Computing - Concepts, Architecture and Challenges By Yashpalsinh Jadeja and Kirit Modi
[19] Cloud Computing Security: From Single to Multi-Clouds By Mohammed A. AlZain, Eric Pardede, Ben Soh and James A. Thom
[20] Security Framework of Cloud Data Storage Based on Multi Agent System By Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah & Masrah Azrifah Azmi Murad
[21] Security and Privacy-Enhancing Multi cloud Architectures Architecture By Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau.

