Study of Security In the hybrid cloud

Anita Patel
B.E. Student
Department of IT-Kirodimal Institute of Technology, Raigarh (C.G.)

Mili Patel
Assistant Professor
Department of IT-Kirodimal Institute of Technology, Raigarh (C.G.)
Email-milipatel02@gmail.com

Prateek Kumar Singh
Lecturer
Department of IT-Kirodimal Institute of Technology, Raigarh (C.G.)
Email-prateek.kitraigarh@gmail.com

ABSTRACT

Cloud Computing is a relatively new paradigm with the potential to transform how IT hardware and software are designed and purchased. Computing is no longer purchased as typical products but delivered as a service over the Internet from large data centers. However, despite the potential benefits associated with the migration of enterprise applications from an in-house data center into a Cloud infrastructure, there are still some issues that hinder the process. Besides well-known benefits, commodity cloud storage also raises concerns that include security, reliability, and consistency. We present Hybrids key-value store, the first robust hybrid cloud storage system, aiming at addressing these concerns leveraging both private and public cloud resources. As cloud technology becomes immensely popular among these businesses, the question arises: Which cloud model to consider for your business? There are four types of cloud models available in the market: Public, Private, hybrid and Community.

Keywords:

Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Cloud Computing, Cloud Security.

II. INTRODUCTION

Today many enterprises are increasingly turning to hybrid clouds, allowing them to combine the benefits of building private and public clouds as well as leveraging existing IT infrastructure to cut costs, maximize value and modernize the way IT services are delivered. Hybrid clouds are formed when private and public clouds are closely integrated, delivering IT services with the security, control and agility users demand. Citrix XenDesktop and XenApp have been redesigned as cloud ready solutions for delivering both applications and desktops on any type of cloud infrastructure by integrating with any virtual infrastructure technology, storage infrastructure and complex network topologies to deliver a single, unified platform. XenDesktop and XenApp now enable enterprise IT to build common service delivery architecture for all Windows apps and desktops leveraging common policies and tools that simplify deployment and management. By delivering Windows apps and desktops as a cloud-like service, XenDesktop and XenApp can handle multiple versions and instances of both Windows Server and desktop operating systems from a single platform. XenDesktop and XenApp are built to leverage any virtual infrastructure or cloud management platform. Provides the right environment for the right workload at the right time

- Bridges the divide between enterprise IT and line of business.
- Expedites building of new revenue-generating products and services.
- Eliminates the need for additional CAPEX in favor of an OPEX approach.
- Improves resource utilization with consistent and predictable SLAs.
- Simplifies and standardizes IT infrastructure and application platforms.

- Provides consistent and predictable SLAs in our data center or yours.

Benefits of Dimension Data Hybrid Cloud:

- Provides the right environment for the right workload at the right time.
- Bridges the divide between enterprise IT and line of business.
- Expedites building of new revenue-generating products and services.
- Eliminates the need for additional CAPEX in favor of an OPEX approach.
- Improves resource utilization with consistent and predictable SLAs.
- Simplifies and standardizes IT infrastructure and application platforms.
- Provides consistent and predictable SLAs in our data center or yours.

SIGNIFICANE OF STUDY*:*

More and more enterprises are adopting the cloud model for their businesses, whether they are small, mid-sized or large organizations, as cloud computing provides slow cost business solutions to their organizations. It is a well-known fact that every business needs cloud, as the technology has become very popular and accepted world over. Cloud computing has promised tremendous advantages to organizations in terms of cost effectiveness, operational excellence and innovation. The main factor for which enterprises are shifting to cloud is the low cost. This review paper covers the concerns of enterprises in adopting public, private, hybrid, and community clouds for their respective organizations, and lists the differences among them, thus providing a complete idea which model would be better for their enterprises.

OVERVIEW OF CLOUD COMPUTING*:*

Cloud computing has three basic abstraction layers, i.e, system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications) [11]. Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony . Cloud data storage is a technology that uses the internet and central remote servers to maintain data and share the applications. It allows consumer to use applications without installation and access their personal files at any computer with internet access. In general data property analysis system, source and destination file content is compared in the form of bytes. In the cloud environment, data verification is needed for every computation in the storage correctness.

TYPICAL CONCERNS WITH HYBRID CLOUD SECURITY

Cloud computing can be implemented under a variety of service and deployment models, with a notable difference among them in how application and data security is addressed. However, some security concerns are fairly typical for any organization considering cloud adoption: the security of data when migrating to the cloud; the protection of data that resides in the cloud; the potential impact to application availability if data protection and disaster recovery practices fail; the ability to meet the security requirements of application regulatory compliance standards; and whether the IT organization will be
able to maintain enough visibility into and power over their security stance.

PROTECTING DATA IN THE CLOUD - Security concerns among IT organizations choosing to move workloads to the hybrid cloud include controlling access to critical applications and the fear of data breaches or loss. Maintaining the integrity and confidentiality of corporate data in the hands of a cloud service provider raises serious concerns for IT managers who often envision increased risk associated with data that resides in the cloud environment.

MEETING COMPLIANCE REQUIREMENTS - Faced with intensifying regulatory requirements, IT organizations are typically concerned with which kinds of security controls are in place in a hybrid cloud environment, and whether they can satisfy auditors. Some companies are especially reluctant to use the public cloud for customer and other sensitive data because of their security and regulatory compliance concerns.

MAINTAINING CONTROL OF THE DATA - When corporate and customer data is no longer stored in an onsite data center, IT managers need to know that they will still have control of the data. Although security and privacy concerns around hybrid cloud services are similar to those of traditional IT services, they tend to escalate with the fear of external control over organizational assets and the potential for mismanagement of those assets.

BLUELOCK'S SECURE HYBRID CLOUD SERVICES

Although security is one of the biggest concerns for companies considering cloud adoption, Bluelock's innovative architecture and heightened emphasis on security provides organizations the assurance they need no matter what type of workloads and data they choose to migrate to the cloud hosting environment. With extensive cloud security expertise, Bluelock can help organizations begin to take strategic steps toward a logical public or hybrid cloud business model that meets their unique business and IT requirements.

SECURITY REQUIREMENTS BY CLOUD MODEL

Security Requirement	Private Cloud	Commodity Cloud	Bluelock Virtual Datacenters
Data in motion - encrypted	N/A	Yes	Yes
Audits and certifications	Internal	PCI	AT101, can support PCI and HIPAA
ICSA-compliant firewal	Yes	Yes	Yes
Secure remote access	Yes	Yes	Yes
Backup frequency	24 hours	N/A	24 hours
Multi-site failover	No	No	Optional
Mandatory background checks	No	No	Yes
Data at rest - encrypted	Yes	No	Optional

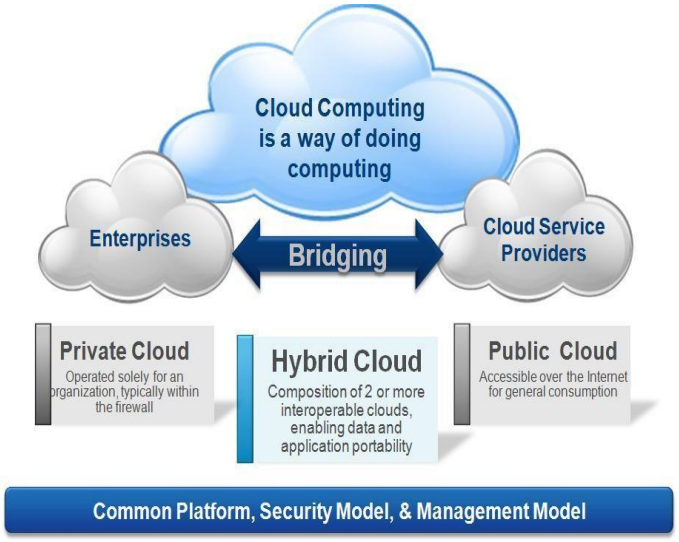

FIG: HYBRID CLOUD MODEL

HYBRID CLOUDS BUILT ON A TRUSTED FOUNDATION:

Hybrid cloud services from VMware and VMware vCloud Air Network Service Provider partners are built on the trusted foundation of VMware vSphereR,the world's leading virtualization platform. You can write, deploy, and manage applications in the cloud the same way you do today, relying on the underlying vSphere platform to provide the same level of security, reliability, and performance you get from your current VMware infrastructure.

III. CONCLUSION:

More and more companies searching for intelligent ways to optimize their IT spend for the greatest flexibility in delivery of services are turning to a hybrid cloud approach. IT executives tasked with exploring their options are finding that the hybrid cloud offers the same or better security for their company's business-critical applications and data, dispelling the myths that have caused them to question the sensibility of moving workloads to the cloud. Leading hybrid cloud providers have the data center infrastructure and expertise to ensure that adequate security is in place to safeguard information in the cloud. The physical, operational, and network processes and controls used in their clouds are commensurate with those used for an organization's internal systems—or better yet, often surpass them. By leveraging the secure hybrid cloud, companies can free up valuable internal IT staff resources, reallocate IT budgets for business innovation, and rest assured that their applications and data will be available 24/7 and will continue to provide competitive advantage.

REFERENCES

1. Worldwide and Regional Public IT Cloud Services 2011– 2015 Forecast, IDC, June 2011.
2. IDG Research, ―CIO Global Cloud Computing Adoption Survey,‖ January 2011.
3. ―Key Issues for Securing Public and Private Cloud Computing, 2011,‖ John Pescatore, Gartner Research. 4. ―Cloud Security Fears Exaggerated, Says Federal CIO,‖ Patrick Thibodeau, Computerworld, July 28, 2011.
(http://news.idg.no/cw/ art.cfm?id=62DE7B46-1A64-67EA-E4E3D0EB9C453EC5)
5. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Stoica, I. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Anita Patel B.E Student
Department of IT-Kirodimal Institute of Technology,
Raigarh (C.G.)

Mili Patel Working as an Assistant Professor,
Department of IT-Kirodimal Institute of Technology,
Raigarh (C.G.)
Email-milipatel02@gmail.com

Prateek Kumar Singh Working as an Lecturer
Department of IT-Kirodimal Institute of Technology,
Raigarh (C.G.)
Email-prateek.kitraigarh@gmail.com