Research Journal of Applied Sciences, Engineering and Technology 7(10): 2172-2174, 2014
DOI:10.19026/ajfst.7.512
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: July 28, 2013 Accepted: August 20, 2013 Published: March 15, 2014

Research Article

Secure Cloud Data Storage Services in the Hybrid Cloud

[1]Mahdi Mollahasani, [1]Raheleh Kooshesh and [2]Mahdiyeh Barzegar
[1]Department of Computer Engineering and Software Engineering,
UCTI-Staffordshire Universiti, Kuala Lumpur, Malaysia
[2]Department of Computer Engineering and Information Technology,
Amirkabir University of Technology, Tehran, Iran

Abstract: Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. The safety of the files depends upon the hosting websites. Lack of control on the data and privacy issues are the biggest obstacles to holding valuable personal and business-critical information in the cloud. Encryption and integrity control is one of the most obvious solutions to address these concerns, however it costs additional complexity of the system and service usage and may impact data access performance. In this study, we will discuss about security challenges in hybrid cloud storage and explain how to preserve security in them.

Keywords: Cloud computing, encryption, hybrid cloud, leveraging a hybrid model, secure cloud, secure storage, storage service

INTRODUCTION

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models Such composition expands deployment options for cloud services, allowing IT organizations to use public cloud computing resources to meet temporary needs This capability enables hybrid clouds to employ cloud bursting for scaling across clouds.

Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization only pays for extra compute resources when they are needed.

Goal of this study is explanation of Security in cloud data Storage in hybrid cloud because Hybrid cloud storage is becoming ever more popular, as organizations look to take advantage of the benefits of public and private clouds while mitigating the drawbacks. Different types of cloud are shown in Fig. 1. Public clouds offer a pay-as-you go financial model as well as easy scalability to deal with spikes in demand. A public cloud solution is also very cost-effective, since organizations only pay for what they use. Private clouds are better for larger organizations that require local access, granular control, specific compliance requirements and governance because they demand that organizations have at least some on-site, dedicated infrastructure but security in cloud is very important in cloud computing our data are store in cloud side then everybody such as an attacker can access on that specific date in addition of this part other problem is we can store our data in hybrid cloud then our data will be more risk able for this reason we want to explain some solution for solve those one.

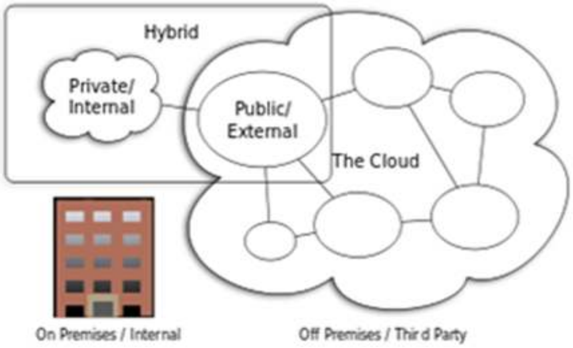

Fig. 1: Cloud computer types

Corresponding Author: Mahdi Mollahasani, Department of Computer Engineering and Software Engineering, UCTI-Staffordshire Universiti, Kuala Lumpur, Malaysia

Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads and use cloud resources from public or private clouds, during spikes in processing demands (Cong *et al*., 2012).

By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

Hybrid clouds lack the flexibility, security and certainty of in-house applications. Hybrid cloud provides the flexibility of in house applications with the fault tolerance and scalability of cloud based services (Robert Koletka, 2011).

Hybrid cloud solutions can strike a balance between the cost-effectiveness and scalability of a public cloud and the greater control and security of a private cloud. With hybrid cloud storage, organizations may position frequently accessed data or extremely sensitive data on-site for rapid, secure access, writing for data storage consulting firm Neovise. Data that is needed less often, such as archived transaction histories or document images, Burns said, is stored in a public cloud where it can still be quickly and transparently accessed when needed.

HYBRID CLOUD STORAGE SOLUTIONS KEY CHALLENGES

Hybrid cloud storage solutions key challenges offer hitherto unparalleled flexibility and capacity-on-demand benefits. But, cloud storage also poses some difficult challenges that have limited its uptake so far. These include issues around latency as well as the security and reliability of data transport that arise when storage resources are located remotely. Consequently, hybrid cloud solutions for storage have emerged, seeking to overcome these issues by locating some storage resources locally and effecting reliable and secure transport to the cloud.

Hybrid cloud storage is a method of deploying storage that uses local and cloud-based storage resources. These hybrid cloud solutions can be contrasted with purely local storage, where all hardware sits within the customer data center, or a completely cloud-based solution, where all resources sit in the cloud and are accessed across the Internet.

Hybrid cloud storage consists of an appliance provided by the vendor in conjunction with a connection to remote storage resources. The implementation appears to the user as a single entity presenting disk storage. The appliance may be supplied as physical hardware or as a virtual machine and hybrid cloud storage implementations can offer both file and block protocols (Miller *et al*., 2002).

The most obvious benefits to cloud data storage are capacity and the ability to scale. There are, however, a number of challenges in delivering storage resources remotely across the Internet between a cloud service provider and the customer. These include:

Latency: Latency in this context is the time taken for data to be transmitted over the Internet between the provider and the customer. Higher latency values mean longer response times and lower throughput of data. In local SAN environments buffers in the array and host enable multiple blocks of data to be “on the wire” at any one time and response times are typically 10 msec or less, with only a small part of that being the fabric transport time (whether Ethernet or Fiber Channel). As latency increases-such as in transport over long distances to and from the cloud provider-throughput drops dramatically as less data is in transit across the network.

Security: Security means the use of secure transfer protocols and authentication of user requests. Cloud storage is widely perceived as being less secure than retaining data in-house. There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers.

Reliability: Data travelling between a cloud storage provider and the host needs to be moved reliably. Reliable delivery means ensuring data transfers have completed successfully and acknowledgements received in the correct order.

In local storage, the protocols used to ensure reliable delivery of data, but these cannot be used for transport to and from the cloud. Within the data center, Fiber Channel, iSCSI and NFS/CIFS are dominant, but they are not suited for long-distance operation. Fiber Channel is a narrated protocol, so it relies on IP for routing over disparate networks or requires dark fiber or other dedicated expensive connections. CIFS and NFS is both ”chatty” protocols in that they require a large management overhead; CIFS, for example, requires confirmation of each block of data transferred before transferring the next. Where a network has large latency issues, performance with CIFS can be particularly slow (Jinhui *et al*., 2010).

SOLUTIONS TO RESOLVE CHALLENGES IN HYBRID CLOUD

Hybrid cloud storage addresses issues related to cloud data storage in the following ways:

Latency: Hybrid cloud solutions overcome latency issues with caching data locally and using WAN optimization techniques to reduce data traffic. For read requests, this often means the use of a least recently used, or LRU, algorithm, where the most recently accessed data stays in cache and is expired or replaced with newer data over time. For write requests, the appliance may choose to store data locally and then write in bursts to improve traffic flow. It is important when evaluating hybrid cloud products to ensure you understand the write caching process used for data loss could occur if the appliance or Internet connection fails.

Security: A hybrid cloud storage appliance provides security at a number of levels. Firstly, it provides secure access to the cloud storage provider, based on the provider's authentication mechanism. Secondly, it encrypts data in transit across the network (using protocols such as SSL/TLS). Thirdly, it encrypts data at rest within the cloud provider's storage environment.

Reliability: Appliances provide standard protocol support within the client data center, including NAS protocols (CIFS and NFS) and block protocols such as iSCSI. But, these are difficult or impossible to use for data to/from the cloud. So, appliances convert local protocol instructions to a web-based APIs such as Representational State Transfer (REST), which use simplified I/O commands that perform read, write and delete of data stored as objects. In addition, data integrity is maintained by storing metadata containing write time stamps with the content itself. The time stamps allow data to be reconstructed in the correct order in the event of a failure (Nepal, 2011).

LEVERAGING A HYBRID MODEL ACCOMPLISHES SEVERAL GOALS

It provides a clear use case for public cloud computing. Specific aspects of existing IT infrastructure (say, storage and compute) occur in public cloud environments and the remainder of the IT infrastructure stays on premise. Take the case of business intelligence in the cloud-although some people promote the migration of gigabytes of operational data to the cloud, many others find the hybrid approach of keeping the data locally and the analytical processing in the cloud to be much more practical.

Using a hybrid model is a valuable approach to architecture, considering you can mix and match the resources between local infrastructure, which is typically a sunk cost but difficult to scale, with infrastructure that's scalable and provisioned on demand. You place the applications and data on the best platforms and then span the processing between them.

The user of hybrid computing acknowledges and validates the fact that not all IT resources should exist in public clouds today and some may never exist in public clouds. Considering compliance issues, performance requirements and security restrictions, the need for local is a fact of life. This experience with the hybrid model helps us all get better at understanding what compute cycles and data have to be kept local and what can be processed remotely (Kaufman, 2009).

Of course there are cloud providers that already have their eye on leveraging a hybrid model. These new kids on the block even provide management and operating system layers specifically built for hybrid clouds. However, the majority of public cloud providers are religious about pushing everything outside of the firewall (after all, that's where they are). They need to be careful that their zealotry doesn't turn off potential cloud converts.

CONCLUSION

Over time, it became clear that hybrid cloud computing approaches have valid roles within enterprises as IT tries to mix and match public clouds and local IT assets to get the best bang for the buck. Now it's the cloud computing providers who are pushing back on hybrid cloud computing, as they instead try to promote a pure public cloud computing model.

REFERENCES

Cong, W., Q. Wang, K. Ren, N. Cao and W. Lou, 2012. Toward secure and dependable storage services in cloud computing. IEEE Transactions on Serv. Comput., 5(2): 220-232.

Jinhui, Y., S. Chen, S. Nepal, D. Levy and J. Zic, 2010. TrustStore: Making amazon S3 trustworthy with services composition. Proceeding of 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid). Melbourne, VIC, pp: 600-605.

Kaufman, L., 2009. Data security in the world of cloud computing. IEEE Secur. Priv., 7: 61-64.

Miller, E.L., W.E. Freeman, D.D.E. Long and B.C. Reed, 2002. Strong security for network-attached storage. Proceeding of Conference on File and Storage Technologies (FAST), pp: 1-13.

Nepal, S., 2011. DIaaS: Data Integrity as a Service in the cloud. Proceeding of IEEE International Conference on Cloud Computing (CLOUD), Washington, DC., pp: 308-315.

Robert Koletka, A.H., 2011. An architecture for secure searchable cloud storage. Proceeding of Information Security South Africa (ISSA). Johannesburg, pp: 1-7.