CLOUD COMPUTING: A REVIEW PAPER

Amrita Parashar*

Mr. Dheeraj Pal*

ABSTRACT :

A cloud storage system, consisting of a group of storage servers, provides long storage services over the net. General coding schemes protect information confidentiality, however also limit the functionality of the storage system as a result of a couple of operations are supported over encrypted information. Constructing a secure storage system that supports multiple functions is difficult once the storage system is distributed and has no central authority. Although considerable progress has been made, more research needs to be done to address the multi-faceted security concerns that exist within cloud computing. Security issues relating to standardization, multi-tenancy, and federation must be addressed in more depth for cloud computing to overcome its security hurdles and progress towards widespread adoption. The distributed storage system not only supports secure and strong information storage and retrieval, however also lets a user forward his information within the storage servers to a different user while not retrieving the info back. We have a tendency to analyze and counsel appropriate parameters for the amount of copies of a message sent to storage servers and therefore the number of storage servers queried by a key server. These parameters permit additional flexible adjustment between the amount of storage servers and robustness. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well.

***KEY WORDS**: IaaS, PaaS, SaaS.*

[*] Department of Computer Science Engineering, Amity University Madhya Pradesh, Gwalior.

1. Introduction

Cloud computing is a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables cloud services.

2. Architecture

The security architecture and functions highly depend on the reference architecture, and this paper shows the reference architecture and the main security issues concerning this architecture. The main key feature and sercices of cloud computing architecture are:

1. Infrastructure-as-a-Service (IaaS)
2. Platform-as-a-Service (PaaS)
3. Software-as-a-Service (SaaS).

IaaS-Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Iaas include various types of components and characteristics like Utility computing services and billing model, Dynamic scaling, Desktop virtualization, Internet connectivity, policy based services etc.

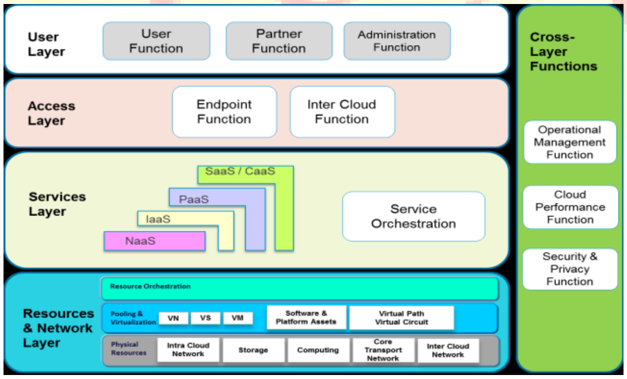

Figure1 cloud storage architecture

Cloud computing data centers are modeled upon a simple design-for-failure infrastructure. They use low-cost, purpose built, scalable solutions, including servers, storage systems and networking products, while still utilizing standard delivery models and massive economies of scale. Cloud computing data centers, however, These products are too expensive and include features that do not meet the cloud’s unique data center environment and application requirements.

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed it's sometimes referred to as utility computing. Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS). Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS.

PaaS– PaaS is a set of software and development tools hosted on the provider's servers. Google Apps is one of the most famous Platform-as-a-Service providers. This is the idea that someone can provide the hardware (as inIaaS) plus a certain amount of application software - such as integration into a common set of programming functions or databases as a foundation upon which you can build your application. Platform as a Service (PaaS) is an application development and deployment platform delivered as a service to developers over the Web. Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from income portability problems. Overall expenses can also be minimized by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

SaaS- Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world.

SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution. Saas model having several Benefits like easier administration, Global accessibility, easier collaboration, compatibility etc.

4. Cloud Computing Models-

4.1Public Cloud-A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. The main benefits of using a public cloud service are:

- Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
- Scalability to meet needs.
- No wasted resources because you pay for what you use.

Hybrid Cloud
Private Clouds
Public Clouds

4.2 Private Cloud- Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation.

Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2C) or Simple Storage Service (SSS).

4.3 Hybrid Cloud- A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data.

The hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT.

To be effective, a management strategy for hybrid cloud deployment should address configuration management, change control, security, fault management and budgeting. Because a hybrid cloud combines public cloud and private data center principles, it's possible to plan a hybrid cloud deployment from either of these starting points. Picking the better starting point, however, will make it easier to address business goals.

A primary goal of a hybrid cloud deployment should always be to minimize change. No matter how similarly a public and private cloud are matched, design differences will inevitably exist.

The greater the differences between the cloud environments, the more difficult it will be to manage multiple clouds as a single entity.

4.4 Community Cloud- Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3).

5. Threats for Cloud Service Providers

5.1 Responsibility Ambiguity

Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user).

5.2 Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

5.3 License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a “clouded” license management scheme which allows to pay only for used licenses may cause software use conflicts.

5.4 Service Unavailability

Availability is not specific to cloud environment. However, because of the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers much more possibilities for an attacker. A typical Denial of Service attack on one service may clog the whole cloud system.

5.5 Unsecure Administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment.

However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

5.6 Data Unreliability

Data protection includes access to data for the confidentiality as well as its integrity. Cloud service users have concerns about how providers handle with their data, and whether their data is disclosed or illegally altered. Even if the cloud service user trust is not in the central of cloud security, it is a major marketing differentiator for a cloud service provider to advance the migration of IT system to cloud environment.

6. CLOUD COMPUTNG SECURITY ISSUES

Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

6.1 Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

6.2 Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

6.3 Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the

CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

6.4 Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" . On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

6.5 Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

6.6 Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring .

6.7 Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

7. CONCLUSION

Cloud Storage with a great deal of promise, aren't designed to be high performing file systems but rather extremely scalable, easy to manage storage systems. They use a different approach to data resiliency, Redundant array of inexpensive nodes, coupled with object based or object-like file systems and data replication (multiple copies of the data), to create a very scalable storage system. Designing storage architectures for emerging data-intensive applications presents several challenges and opportunities. Tackling these problems requires a combination of architectural optimizations to the storage devices and layers of the memory/storage hierarchy as well as hardware/software techniques to manage the flow of data between the cores and storage. While there are issues of non-uniformity across cloud vendors there is a requirement to provide uniform user interfaces and seamless integration with the mainstream desktop and server computing. Moreover, since a cloud infrastructure is a distributed system, storage facilities may be designed like the distributed file system.

8. REFERENCES

［1］. Jiyi WU1,2, Lingdi PING1, Xiaoping GE3,Ya Wang4, Jianqing FU1, 2010 International Conference on Intelligent Computing and Cognitive Informatics, ―Cloud Storage as the Infrastructure of Cloud Computing‗

[2]. Storage Networking Industry Association. Cloud Storage for Cloud Computing, Jun.2009.

[3]. Curino, Jones, Popa, Malviya, Wu, Balakrishnan and Zeldovich, Relational Cloud : A Database-as-a-Service for the Cloud, 2010

[4]..http://www.infostor.com/index/articles/display/0442659564/articles/Infostor/backup and_recovery/cloud storage/2010/march-2010/sniadevelops_standards.html

[5]. Storage Networking Industry Association. Cloud Storage Reference Model,Jun.2009

[6].http://searchsmbstorage.techtarget.com/feature/Understanding-cloudstorage- services-A-guide-for-beginners