International Journal of Information Technology and Knowledge Management
July-December 2010, Volume 2, No. 2, pp. 345-349

ANALYSIS OF SECURITY ISSUES AND PERFORMANCE ENHANCEMENT IN CLOUD COMPUTING

Herminder Singh[1] & Babul Bansal[2]

The ability to scale a web application or website is tied directly to understanding where the resource constraints lie and what impact the addition of various resources has on the application. Unfortunately, architects more often than not assume that simply adding another server into the mix can fix any performance problem and security issues. Cloud is a platform shuffle that enables a fierce and contentious debate on the issues of security and performance surrounding how to secure information and instantiate trust in an increasingly open and assumed-hostile web operating environment. When you start adding new hardware/update existing hardware in a web cloud, the complexity starts increasing which affects performance and hence security. Here we will define the algorithms to keep both performance and data secure but flexible enough to allow for expandability.

Keywords: Cloud Computing, Cloud Platform, Cloud Infrastructure, Cloud Security.

1. Introduction

The designers of security solutions have consistently debated the tradeoffs between levels of security and the resulting performance. When computational resources are provided to the existing system, one of the main challenges that computing community face is leaked security and deteriorating performance. "Cloud computing" takes hold as 69% of all internet users have either stored data online or used a web-based software application. Growths in the number of applications and the volume of data that must be managed have made data centers to be as wide as possible, with no end in sight. But if cloud computing is going to meet enterprise needs for confidentiality of customer data and compliance with legal directives, it will have to provide increased levels of security to support more sensitive enterprise applications. To date, most of the public cloud-oriented applications have been consumer-centered applications built on commoditized data storage and transaction processing. At this initial stage, the applications and data being processed in clouds are predominantly non-sensitive, and the cloud services offer minimal or only generally available security. In a web application, you don't simply add more capacity to the system just because your CPUs have hit 90% utilization. It's important to be able to answer the question, "What does supporting this additional load get me?" Knowing the value of the demand on your system will help answer that question.

[1]Sr. System Analyst, Zelite Solutions (Development/Training Division), Haryana, India

[2]Asst. System Analyst, Zelite Solutions (Development/Training Division), Haryana, India

Email: [1]hermindersingh13@gmail.com, [2]babul.bansal@yahoo.com

2. Cloud Computing

Cloud computing is a model for enabling convenient, 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. This cloud model promotes availability and is composed of three service models, and four deployment models. However "Cloud computing" is a difficult term to explain to most; even to technologists and IT professionals, the concept of computing in the cloud is a wide and generic term for many specific areas within online environment. The "cloud" is defined as the Internet surrounding every part of our daily lives, similar to the clouds in the sky. However many new enterprise related buzzwords have evolved from the original "computing in the cloud" concept; "Software-as-a-Service", "Software + Services" which has evolved as a more Microsoft related term, and "social-media" which is a cornerstone in social networking and development. Whilst a common misconception for cloud computing is merely storage space on the Internet, the cloud offers many services, infrastructure benefits and scalability which may not be possible within ordinary local-area enterprise networks. When cloud storage is used as the primary location of files and documents, a certain trust is left in the hands of the storage provider to ensure certain steps are taken to prevent data loss and maintain the integrity of the file system; enabling maximum uptime, reducing downtime and sustain the highest levels of physical protection and data security.

When something affects cloud storage, things can go disastrously wrong for many end users. Whilst data which is stored in the cloud isn't actually stored in the cloud; rather

a Data Center housing hundreds of servers and thousands of networking cables, physical disasters are one of the greater threats to the cloud.

As physical disasters go, some will affect the entire cloud, or entire datacenter if you think geologically or physically, and some will affect portions or individual sections. Natural disasters are a great concern to those who run and use cloud computing services. As many natural disasters are unpredictable, from floods to earth tremors, volcanoes and tsunamis, recovering from these disasters are often impossible. Preventing disasters from affecting the cloud itself is the only realistic thing the staff, management and planners can foresee. Nobody would build a datacenter; let alone any Business Venture, Government building, School or Hospital, or any building or structure of importance in a geographic location where an active or dormant volcano lies, e.g. In case of cloud downtime or event which causes the cloud to fail, a backup solution is often used in an alternate location. This ensures a constant stream of data being backed up to an alternate datacenter, away from any potential natural disaster, but keeping data secure and maximizing authorized accessibility.

3. ARCHITECTURE

After analyzing WBS (Web Banking System), Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud components communicating with each other over application programming interfaces, usually web services. This closely resembles the Unix philosophy of having multiple programs doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts.

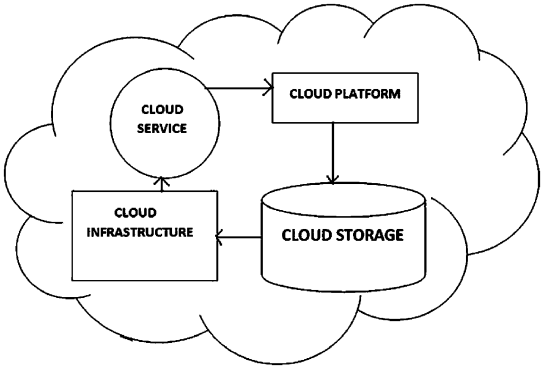

Fig.1: Architecture of Cloud

Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or users.

Security is the #1 challenge seen related to Cloud Computing according to our architecture.

- The main security concerns include performance, reliability compliance, privacy in interoperability and visibility under virtualization.
- The Good News: Since Security is seen as such a major issue, it is getting much attention. This attention is resulting in Security-related benefits such as greater segmentation and better logging and performance is another issue if we change the level of security in the Cloud.

With increasing Business complexity, organizations are seeking innovative business models and specialized technologies to cater to customer demands. Cloud computing technologies can provide organizations competitive advantage in the market, cost reductions, higher margins, simplified maintenance and management of applications across the enterprise, greatly extended scalability, agility, high availability, automation, large data storages and reliable backup mechanisms.

By using Cloud Computing environments, organizations can focus on their core business as opposed to concerning themselves about infrastructure scalability. Organizations may explore use of cloud computing initially for better performance through peak demand periods but eventually adoption could spread to other areas.

4. SERVICE MODELS

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications 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). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is 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. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

5. DEPLOYMENT MODELS

Private Cloud: The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community Cloud: The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud: The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid Cloud: The Cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

6. CURRENT VIEW

Critics argue that Cloud Computing is not secure enough because data leaves companies' local area networks.

It is up to the clients to decide the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Salesforce, Amazon and Google are currently providing such services, charging clients using an on-demand policy. Statistics suggest that one third of breaches are due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/ middleware security patches faster because of higher availability of staff and resources.

According to cloud vendors, most thefts occur when users with authorized access do not handle data appropriately. Upon a logout from the cloud session, the browser may be configured to delete data automatically and log files on the vendor side indicate which user accessed what data. This approach may be deemed safer that storing data on the client side. There are some applications for which Cloud Computing is the best option. One example is the New York Times using Amazon's cloud service to generate PDF documents of several-decade old articles. The estimated time for doing the task on the Times' servers was 14 years, whereas the cloud provided the answer in one day for a couple hundred dollars.

However, the profile of the companies that currently use the Cloud Technology includes Web 2.0 start-ups that want to minimize material cost, application developers that want to enable their software as a service or enterprises that are exploring the cloud with trivial applications. The fact that Cloud Computing is not used for all of its potential is due to a variety of concerns. The following surveys the market in terms of continuous innovation, academia and industry research efforts and Cloud Computing challenges.

7. PERFORMANCE ISSUES

Everybody seems to be talking loud about Cloud Computing nowadays. But the recently reported outages at Salesforce, Amazon and Google has made us think otherwise and wonder if the cloud is really ready to meet all the hype and attention its getting. No doubt, there are cost savings related to licensing, maintenance and application / server management. But does this ensure that your end users are getting the online experience you want them to have?

Many Cloud Computing providers provide custom built management consoles or control panels for managing server resources. These consoles provide customers with availability statistics and status messages in the event of significant outages that impact end users.

8. IMPROVE PERFORMANCE ISSUES-EQUATIONS

The first and foremost thing to keep in mind is that even you are hosting on a Cloud or have a SAAS app running somewhere, your end user expectations are no different then the regular client server application. So in a generic sense User Acceptance Testing is not much different then testing on a Client Server Architecture.

Remember web based application environment in the cloud is a jigsaw puzzle of pieces. At the core you have your virtual hardware followed by your operating system. Each of your servers is then configured differently depending on its specific duty. You may have application servers, web servers, search servers, database servers etc. Each of these servers needs to be monitored from several points of view - both internally and externally.

Though you don't have direct access to performance monitoring like in a Client Server Architecture but still you can follow following steps to make sure your users are getting the experience you want them to:

Algorithm at the server side:

Notation:

T_{low}: Time interval for the slow mode

T_{high}: Time interval for the fast mode

T_{fixed}: Fixed time interval for the super-fast mode

T_{th}: Threshold time

c_{size}: Cloud size

id_r: id of Resources

gid: group id of Resources

D: the set of Resources

IR_i: the set of resource ids

$Client_{th\text{-}low}$: the lower threshold number of clients for the cloud

$Client_{th\text{-}high}$: the higher threshold number of clients for the cloud

R_{data}: an id list of resources that a client has requested from the cloud

$R_{broadcast}$: an id list of data items that the server received in the last IR interval; initialized to be empty

$R_{performance}$: Performance of cloud and timestamp for all resources

S_r: Start Resources

S_t: Stop Resources

Performance: $S_r(n)_t$ .. $S_t(n)_t$

$Performance_i$: Performance issue = $S_r(n)_t$-$S_t(n)_t$

(A) Slow Mode (Cloud Performance)

At interval time T_i, construct IR_i, as follows-

$IR_i = \{[gid, t] \mid (gid \bullet \{IR\}) \wedge ((T_i\text{-}T_{low} \times w) < t < Ti)\}$;

Broadcast IR_i, T_{low};

Receive R_{data};

For every $id_r \bullet R_{data}$ broadcast $d \bullet D$ {

Update $Counter_{client}$

Execute Step B if T_{th} is reached and

$Counter_{client} > Client_{th\text{-}low}$;

Execute Step C if T_{th} is reached and

$Counter_{client} > Client_{th\text{-}high}$

}

(B) Fast Mode (Cloud Performance)

At interval time T_i, construct IR_i, as follows-

$IR_i = \{[id_r, t] \mid (id_r \bullet \{IR\}) \wedge ((T_i\text{-}T_{high} \times w) < t < Ti)\}$;

Broadcast IR_i, T_{high};

Receive R_{data};

For every $id_r \bullet R_{data}$ broadcast $d \bullet D$ {

Update $Counter_{client}$

Execute Step A if T_{th} is reached and

$Counter_{client} < Client_{th\text{-}low}$;

Execute Step C if T_{th} is reached and

$Counter_{client} > Client_{th\text{-}high}$

}

(C) Super fast Mode (Cloud Performance)

At interval time T_i, construct IR_i, as follows-

$IR_i = \{[d, t] \mid (d \bullet D) \wedge ((T_i\text{-}T_{fixed} \times w) < t < Ti)\}$;

Send IR_i, T_{fixed} point to point;

Execute Step B after T_{fixed} is elapsed;

9. RESULTS

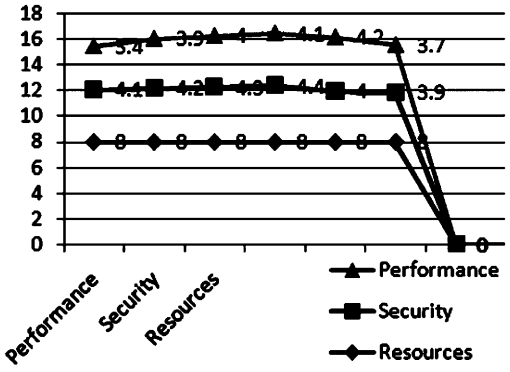

Fig.1: General Graph of Performance of a Cloud

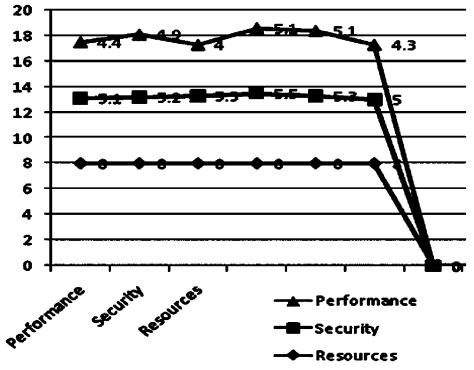

Fig.2: Graph in Slow Mode of Performance of a Cloud

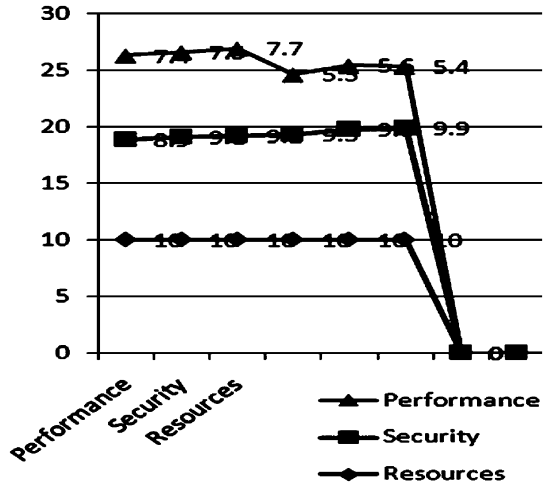

Fig.3: Graph in Fast Mode of Performance of a Cloud

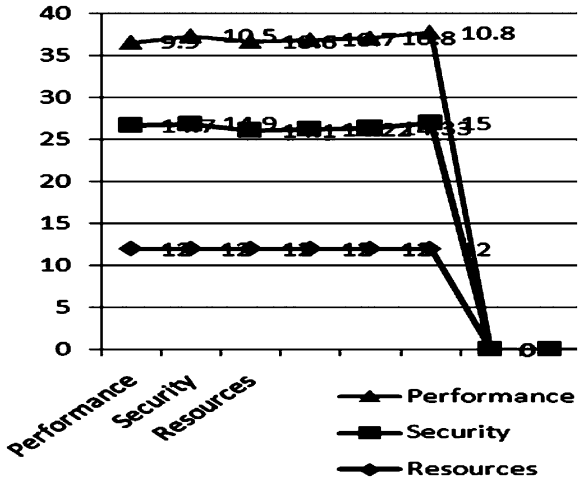

Fig.4: Graph in Super Fast of Performance of a Cloud

10. CONCLUSION

In conclusion, natural or physical disaster to the datacenter which houses the cloud in hardware form would be the main matter of concern to the company or those involved in the running of the datacenter. On the other hand, regardless of company size or volume and magnitude of the cloud, from the findings discussed within this paper, network or computing downtime is the most detrimental effect to have on the end user. If you have no connectivity to the Internet or from the Internet to the datacenter where the cloud is hosted, you cannot access what you need to and the entire cloud concept is therefore made redundant.

11. FUTURE WORK

For those deploying software out in the Cloud, scalability is a major issue.

1. The need to marshal resources in such a way that a program continues running smoothly even as the number of users grows.
2. It's not just that servers must respond to hundreds or thousands of requests per second.
3. The system must also coordinate information coming from multiple sources fast, not all of which are under the control, of the same organization.

With these equations there is a possibility that the security can be breached, but the performance will be increased according to our scenario when the number of users are increased. In future we want to design a protocol which will be more secure and the performance of the cloud will increase.

REFERENCES

[1] Draft NIST Working Definition of Cloud Computing v15, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[2] Foley, M., J., 2008. Microsoft 2.0: How Microsoft Plans to Stay Relevant in the Post-Gates Era. Indianapolis: Wiley.

[3] Whittaker, Z., 2008. Egnyte: using and Sustaining Enterprise 2.0 | Enterprise Alley | ZDNet. [Online]. Available at: http://blogs.zdnet.com/enterprisealley/?p=289 [Accessed 6th November 2008].

[4] Weiss, A., 2007. Computing in the Clouds, NetWorker, 11(4), pp. 16-25.

[5] Togio, J., W., 2002. Disaster Recovery Planning: Preparing for the Unthinkable. 3rd ed. New York: Prentice Hall.

[6] Beard, H., 2008.Cloud Computing Best Practices for Managing and Measuring Processes for On-Demand Computing, Applications and Data Centers in the Cloud with SLA's. Amazon.com: Emereo.

[7] [Mills09] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies",2009 http://news.zdnet.com/2100-9595_22-264312.html.

[8] http://coolwebdeveloper.com/2009/03/is-cloud-computing-reliable-enough-how-9) to-monitor-downtime-or-poor-performance-of-the-cloud/.

[10] IsecT Ltd., 2004. Notice Board Technical Briefing: securing Physical Access and Environmental Services for Datacenters. [E-book] Available at:http:// www.noticebored.comNB_tech_briefing_on_datacenter_security_SAMPLE.pdf [Accessed 9th November 2008].