International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-1 Number-1 Issue-1 September 2011

Analytical Approach for Analyzing Trusted Security System for Data Sharing in Cloud Environment

Anand Srivastava[1], Surendra Mishra[2], Pankaj Kawadkar[3]
M.Tech Scholar, Dept. of Computer Science, SSSIST Sehore,India[1]
Head, PG Dept. of Computer Science, SSSIST Sehore,India[2]
HOD, MCA, SSSIST Sehore,India[3]

Abstract

Cheap, seemingly unlimited computing resources that can be allocated almost instantaneously and pay-as-you-go pricing schemes are some of the reasons for the success of Cloud computing .In this paper we discuss few aspects of cloud computing and also there area. Cloud computing has been acknowledged as one of the prevailing models for providing IT capacities. The computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services. In this paper we discuss several of the aspects of cloud computing which includes security in cloud computing, usage of cloud computing and how we can interact in the interconnection domains.

Keywords

Cloud Computing, Security, Data Sharing, Trusted Model

1. Introduction

Cloud computing has opened up a new frontier of challenges by introducing a different type of trust scenario. Today, the problem of trusting cloud computing is a paramount concern for most enterprises. It's not that the enterprises don't trust the cloud providers' intentions; rather, they question cloud computing capabilities. Yet the challenges of trusting cloud computing don't lie entirely in the technology itself. The dearth of customer confidence also stems from a lack of transparency, a loss of control over data assets, and unclear security assurances.

Cloud Computing services as defined above are best exemplified by the Amazon Web Services (AWS) [1][2] or Google AppEngine [3][4]. Both of these systems exhibit all eight characteristics as detailed below. Various companies are beginning to offer similar services, such as the Microsoft Azure Service [5], and software companies such as VMware [6] and open source projects such as UCSB Eucalyptus [7][8] are creating software for building a cloud service. Cloud computing refers to the provision of computational resources on demand via a computer network. Users or clients can submit a task, such as word processing, to the service provider, such as Google, without actually possessing the software or hardware. The consumer's computer may contain very little software or data, serving as little more than a display terminal connected to the Internet. Since the cloud is the underlying delivery mechanism, cloud based applications and services may support any type of software application or service in use today.

Identifying integrity properties is critical to the effectiveness of any integrity measurement mechanism, because without a good set of integrity properties, the use of such mechanisms can be severely limited. For example, if the integrity properties only cover system call table, a new root kit can manipulate other function pointers to achieve its goal and remain undetected.

In a typical cloud computing scenario organizations run their applications from a data centre provided by a third-party the cloud provider. The provider is responsible for providing the infrastructure, servers, storage and networking necessary to ensure the availability and scalability of the applications. This is what most people mean when they refer to cloud computing i.e. a public cloud.

Cloud computing introduces a whole ecosystem of clients, services and infrastructure, where trust boundaries are moved into realms where physical locations and even ownerships are unknown [9]. The variety of technologies required in clouds makes the overall picture confusing [10]. Within clouds, technology and infrastructure details are abstracted away from the sight of the users; data, resources and software are stored on servers in the cloud, and the users experience the cloud via a remote browser conveyed view.

In this paper we discuss several technical issues related to security concern.We provide here an overview of executing data mining services on grid. The rest of this paper is arranged as follows: Section 2 introduces cloud computing and need of security; Section 3 describes about Trusted Computing and Data Sharing; Section 4 shows the recent scenario; Section 5 describes the challenges. Section 6

describes conclusion and future prospect.

2. Cloud Computing and Need Of Security

Cloud security is a big concern in cloud computing era. We categorized the security concern in We categorize the security concerns as:
Conventional Security
Availability
Third-party data control

Conventional Security
These concerns involve computer and network intrusions attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company.

Availability
These concerns center on critical applications and data being available.

Third-party data control
The legal implications of data and applications being held by a third party are complex and not well understood.
Potential areas of improvement where organizations may derive security benefits from transitioning to a public cloud computing environment include the following:

- Staff Specialization: Cloud providers, just as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Increases in the scale of computing induce specialization, which in turn allows security staff to shed other duties and concentrate exclusively on security issues. Through increased specialization, there is an opportunity for staff members gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties.

- Platform Strength: The structure of cloud computing platforms is typically more uniform than that of most traditional computing centers. Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also profit from a uniform, homogeneous cloud infrastructure, as do system management activities, such as fault management, load balancing, and system maintenance. Many cloud providers meet standards for operational compliance and certification in areas like healthcare.

- Resource Availability: The scalability of cloud computing facilities allows for greater availability. Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents. When an incident occurs, an opportunity also exists to capture information more readily, with greater detail and less impact on production. In some cases, however, such resiliency can have a downside. For example, an unsuccessful distributed denial of service attack can quickly consume large amounts of resources to defend against and cause charges to soar, inflicting serious financial damage to an organization.

- Backup and Recovery: The backup and recovery policies and procedures of a cloud service may be superior to those of the organization and, if copies are maintained in diverse geographic locations, may be more robust. Data maintained within a cloud can be more available, faster to restore, and more reliable in many circumstances than that maintained in a traditional data center. Under such conditions, cloud services could also serve as a means for offsite backup storage for an organization's data center, in lieu of more traditional tape-based offsite storage. However, network performance over the Internet and the amount of data involved are limiting factors that can affect restoration.

- Mobile Endpoints: The architecture of a cloud solution extends to the client at the service endpoint, used to access hosted applications. Cloud clients can be browser-based or applications-based. Since the main computational resources needed are held by the cloud provider, clients are generally lightweight computationally and easily supported on laptops, notebooks, and net books, as well as embedded devices such as

smart phones, tablets, and personal digital assistants.

- Data Concentration: Data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur. Many organizations have already made the transition to support access to organizational data from mobile devices to improve workflow management and gain other operational efficiencies.

There are different scenarios which can access the control from different environments which is shown in Fig 1.The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication that can become unworkable over time. Security Assertion Markup Language (SAML) standard or the OpenID standard are also used for securing the data in shared environment.

A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the extensible Markup Language (XML) for its format. SOAP messages are digitally signed.

Most organizations employ contractors as part of their workforce. Cloud providers are no exception. As with regular employees, the contractors should go through a full background investigation comparable to your own employees. Your cloud provider must be able to provide you with its policy on background checks and document that all of its employees have had a background check performed, according to the policy. Further, you should contractually bind the cloud provider to require the same level of due diligence with its contractor

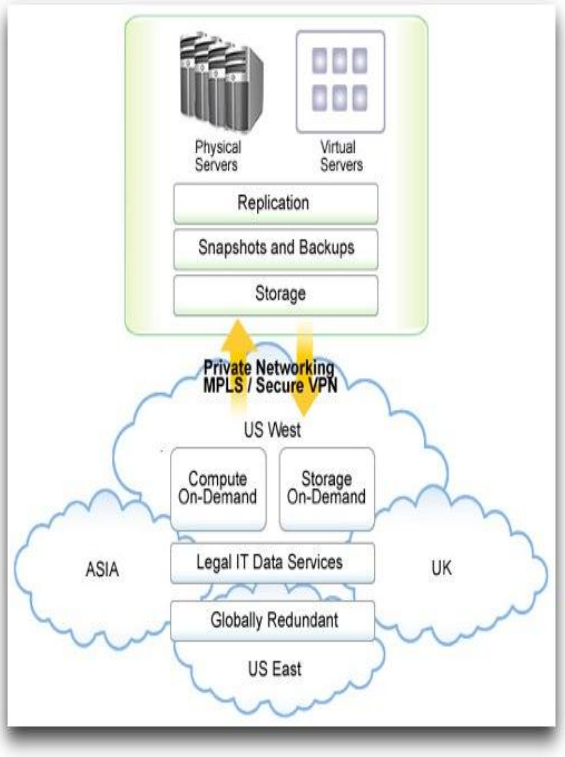

Fig1. Cloud Computing Environment.

3. Trusted Computing and Data Sharing

According to Khaled M. Khantrust means an act of faith; confidence and reliance in something that's expected to behave or deliver as promised. It's a belief in the competence and expertise of others, such that you feel you can reasonably rely on them to care for your valuable assets. Control is another important issue in trust. We trust a system less when we don't have much control over our assets.

We can also see a variation of trust, depending on the ownership of data assets. Alice might trust an online payment system when she pays with her credit card, but she might have less trust in the same system when using her client's card, because preserving her client's interest is one of her business objectives. Trust in cloud computing is related more to preventing a trust violation than to guaranteeing compensation should a violation occur. For most enterprises, a security breach of data is irreparable no amount of money can guarantee to restore the lost data or the enterprise's reputation. The cloud computing trust model thus should focus more on preventing failure than on post-failure compensation.
Looking at cloud computing from both sides now reveals the factors that put information at risk in the cloud. Comparing the findings from both studies reveals that neither the company that provides the

services nor the company that uses cloud computing seem willing to assume responsibility for security in the cloud. In addition, cloud computing users admit they are not vigilant in conducting audits or assessments of cloud computing providers before deployment. They also seem to be frustrated because decisions to use certain applications are made by end-users who may not have the knowledge or expertise to properly evaluate security risks.

4. Recent Scenario

In 2010, Dr. Rao Mikkilineni [10] describes the combination of hardware assisted virtualization and the broadband Internet have taken the Information Technology (IT) hosted managed services to a next level of evolution, where the software applications have become independent of the hardware infrastructure and can be migrated at will.

In 2010, Gansen Zhao et al. [11] aim to construct a system for trusted data sharing through untrusted cloud providers to address the above mentioned issue. The constructed system can imperatively impose the access control policies of data owners, preventing the cloud storage providers from unauthorized access and making illegal authorization to access the data.

In 2010, David Bernstein et al. [12] proposed a blueprint for an Intercloud economy must be architected with a technically sound foundation and topology. As part of the overall Intercloud Topology, they build on the technology foundation emerging for the Intercloud and specifically delve into details of Intercloud security considerations such as Trust Model, Identity and Access Management, governance considerations and so on.

In 2010, Zhidong Shen et al. [13] proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. They propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

5. Challenges

Like internal IT, cloud providers have internal and external threats that can be mitigated or accepted.

Multi-tenancy
As long as the cloud provider builds its security to meet the higher-risk client, then all of the lower risk clients get better security than they would have normally. If you are a bandage manufacturer there is a low risk of being a direct target of malfeasants.

Security Assessment
Over time, organizations tend to relax their security posture. To combat a relaxation of security, the cloud provider should perform regular security assessments. The assessments should be done by someone who is experienced and able to identify issues and fix them.

Security Assessment
Over time, organizations tend to relax their security posture. To combat a relaxation of security, the cloud provider should perform regular security assessments. The assessments should be done by someone who is experienced and able to identify issues and fix them. The report should be provided to each client immediately after it is performed so they know the current state of the overall cloud's security.

Shared Risk
In many instances, your cloud service provider will not be the cloud operator. But it may be providing a value-added service on top of another cloud provider's service. For example, if Software as a Service (SaaS) provider needs infrastructure, it may make more sense to acquire that infrastructure from an Infrastructure-as-a-Service (IaaS) provider rather than building it. These cloud service provider tiers that get built by layering SaaS on top of IaaS, for example, can affect your security. In this type of multi-tier service provider arrangement, each party shares the risk of security issues because the risk potentially impacts all parties at all layers.

Staff Security Screening
Most organizations employ contractors as part of their workforce. Cloud providers are no exception. As with regular employees, the contractors should go through a full background investigation comparable to your own employees. Your cloud provider must be able to provide you with its policy on background checks and document that all of its employees have had a background check performed, according to the policy.

Distributed Data Centres
Disasters are a fact of life. They include hurricanes, tornadoes, landslides, earthquakes and even fibre cuts. In theory, a cloud computing environment should be less prone to disasters because providers can provide an environment that is geographically distributed. But many organizations sign up for cloud computing services that are not geographically distributed.

Physical Security

Physical external threats should be analyzed carefully when choosing a cloud security provider.

Policies
Any organization that says it has never had a security incident is being deceptive or is unaware of the incidents it has had. It is unrealistic to assume a cloud provider will never have an incident. Cloud providers should have incident response policies. And they should have procedures for every client that feed into their overall incident response plan.

Data Leakage
Data leakage has become one of the greatest organizational risks from a security standpoint. Virtually every government worldwide has regulations that mandate protections for certain data types. The cloud provider should have the ability to map its policy to the security mandate you must comply with and discuss the issues. At a minimum, the data that falls under legislative mandates, or contractual obligation, should be encrypted while in flight and at rest.

6. Conclusion and Future Prospect

Cloud computing has been acknowledged as one of the prevailing models for providing IT capacities. The computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services. In this paper we discuss several of the aspects of cloud computing which includes security in cloud computing, usage of cloud computing and how we can interact in the interconnection domains.

In future we concentrate on the real time scenario with their implementation.

References

[1] Amazon Web Services, http://aws.amazon.com.
[2] Murty, James, Programming Amazon Web Services; S3, EC2,SQS, FPS, and SimpleDB, O'Reilly Press 2008.
[3] [Google AppEngine, http://code.google.com/appengine.
[4] Ciurana, Eugene: Developing with Google App Engine, Firstpress(2009).
[5] http://www.microsoft.com/azure/default.mspx.
[6] http://www.vmware.com/technology/cloud Computing.html.
[7] Nurmi D., Wolski R., Grzegorczyk C., Obertelli G., Soman S.,Youseff L., Zagorodnov D.: The Eucalyptus Open-source Cloudcomputing System, Proceedings of Cloud Computing and Its Applications, Chicago, Illinois (2008).
[8] TiViT, "Cloud software program description," http:// www.cloudsoftwareprogram.org/cloud-security.
[9] K. Hwang, "Massively distributed systems: From grids and p2p to clouds." in The 3rd International Conference on Grid and Pervasive Computing, 2008.
[10] Rao Mikkilineni," Theme: Computing Clouds with Telecom Grade "Trust" and Global Interoperability", WETICE 2010.
[11] Gansen Zhao, Chunming Rongy, Jin Liz, Feng Zhangx and Yong Tang," Trusted Data Sharing over Untrusted Cloud Storage Providers", 2nd IEEE International Conference on Cloud Computing Technology and Science 2010.
[12] Bernstein, David, and Deepak Vij. "Intercloud security considerations." In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pp. 537-544. IEEE, 2010.