INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY ISSUES IN CLOUD COMPUTING

BHOUTIK KANERIYA, MANISH SINGH, SANTOSH DESHMUKH, ABHISHEK KANOJIA

Accepted Date: 25/02/2014; Published Date: 01/03/2014

Abstract: The field of cloud computing is still in its early years as far as implementation and usage, partly because it is heavily promoted by technology advancement and is so high resource dependent that researches in academic institutions have not had many opportunities to analyze and experiment with it. However, cloud computing arises from the IT technician's aspiration to add another layer of unification in processing information. At the moment, a general understanding of cloud computing refers to the following concepts: • Network Computing, • Utility Computing, • Software as a Service, • Storage in the cloud, • Virtualization. These refer to a client using a provider's service remotely, also known as in the cloud. Even if there is an existent debate on whether those concepts should be separated and deal with individually, the general agreement is that all those terms could be summarized by the cloud computing umbrella. Cloud Computing is one of the hottest topic discussed today in the field of IT giving many future oriented technological and economical opportunities. Many customers remain hesitant to move their business IT infrastructure completely to this virtual place. Given its recent development and insufficiency of academic published work, many discussions on the topic of cloud security have surfaced from engineers in companies that provide the aforementioned services. This paper introduces the current state of cloud computing, with its development challenges, academic circles and industry research efforts. Further, it describes cloud computing security problems and benefits and showcases a model of secure architecture for cloud computing performance.

Keywords: Security, Cloud Computing

Corresponding Author: MR. BHOUTIK KANERIYA

Access Online On:

www.ijpret.com

How to Cite This Article:

Bhoutik Kaneriya, IJPRET, 2014; Volume 2 (7): 62-72

PAPER-QR CODE

INTRODUCTION

1.1 Overview

Cloud computing is a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software and that's the specialty of CC. As per the definition provided by the National Institute for Standards and Technology (NIST) (Badger et al., 2011), "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". Cloud Computing is an Internet-based development. The cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high quality services from data and software that reside solely on remote data centers. Cloud Computing is a model that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud.presence in almost all walks of human activities. Some of them are online payment of bills, online shopping, booking travelling tickets and even movie tickets online. It is also used for the vast sea of information it provides regarding any topic under the sun by students, professionals, housewives, etc.

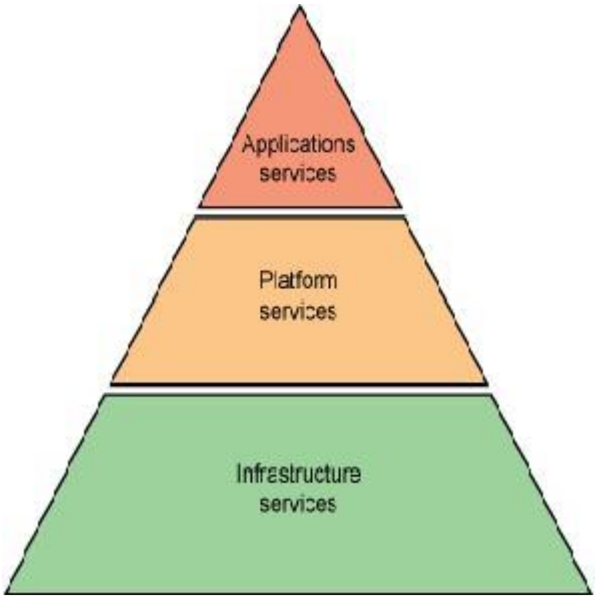
1.2 Cloud Services

The concept based on 3 services; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as well as Web 2.0 and other recent innovative technology trends which rely over the Internet for fulfilling the computing needs of the users.

SaaS: The cloud user, dependent on their contracted services with the cloud vendor will only control certain configuration parameters, whilst the cloud vendor maintains control over applications and infrastructure.

PaaS: The cloud seller controls the cloud infrastructure and runtime environments when the cloud user controls the application.

IaaS: Although a cloud user will have control over their servers with the installed Operating System & Applications with this the cloud offering the cloud vendors will still controls the virtualization infrastructure and at least parts of the network infrastructure.



1.3 Deployment Models in Cloud Computing

Private Cloud- This is referred as cloud for individuals, where everything is with you only the control and ownership. The infrastructure is operated exclusively by the organization who is actual owner of that cloud. The owner has managerial control, and includes only that same organization's data. In this model the access control is with the user or owner.

Community Cloud- This is shared amongst several organizations, either because of a common organizational goal, or in order to pool IT resources. Community clouds may be located within one or more of the community organization’s premises, and will be administered by the community. It is like a group of people with the same interest and fulfilling their requirements with a common source.

Public Cloud- This will usually be owned by a provider organization, which will maintain the cloud facilities in one or more corporate data centers. The administrative control of the cloud resources will therefore reside with the provider, rather than the user.

Hybrid Cloud- This is a composition of two or more of the above deployment models. Hybrid clouds can be used to provide load-balancing to multiple Clouds.

1.4 Advantages of Cloud Computing

Vast Range: Obviously, the biggest facility that cloud computing provides is access to a variety of applications. More importantly, user has neither to install software for this nor face any storage problems.

Flexibility: One of the major benefits of cloud computing is that there is no limitation of place and medium. We can reach our applications and data anywhere in the world, on any system.

Cost-effective: Cloud computing services are easily affordable. User needs not expend on hardware and software systems.

Synchronization and Integrity: Business people can share their data or documents on internet and at one place. They are independent of carrying any specific hardware or software with them.

1.5 Disadvantages of Cloud Computing

Dependency: Among certain limitations of cloud computing is users' dependency on the provider. Risk and Insecurity: Cloud computing services mean taking services from remote servers. User doesn't have control over their software. Also, there is always insecurity regarding stored documents. Nothing can be recreated if their servers go out of service.

Migration Problems: In case the user has to switch to some other provider, there are migration issues. It's not easy to transfer huge data from one provider to the other.

1.6 Security Issues

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

Privileged user access

Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

Regulatory compliance

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner. [5]

Data location

When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises. [5]

Data segregation

Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says. [5]

Recovery

Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a failure. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

Investigative support

Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers

Long-term viability

Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. “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,” Gartner says.

2. ARCHICTECTURE OF CLOUD COMPUTING

In this section, we present a top-level architecture of cloud computing that depicts various cloud service delivery models. Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources (CSA Security Guidance, 2009). These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on- demand utility-like model of allocation and consumption. Cloud services are most often, but not always utilized in conjunction with an enabled by virtualization technologies to provide dynamic integration, provisioning, orchestration, mobility and scale.

While the very definition of cloud suggests the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of cloud. This is often purposely done in an attempt to inflate or marginalize its scope. Some examples include the suggestions that for a service to be cloud-based, that the Internet must be used as a transport, a web browser must be used as an access modality or that the resources are always shared in a multi-tenant environment outside of the “perimeter.” What is missing in these definitions is context.

From an architectural perspective, given this abstracted evolution of technology, there is much confusion surrounding how cloud is both similar and different from existing models and how these similarities and differences might impact the organizational, operational and technological approaches to cloud adoption as it relates to traditional network and information security practices. There are those who say cloud is a novel sea-change and technical revolution while other suggests it is a natural evolution and coalescence of technology, economy and culture. The real truth is somewhere in between.

There are many models available today which attempt to address cloud from the perspective of academicians, architects, engineers, developers, managers and even consumers. The architecture that we will focus on this chapter is specifically tailored to the unique perspectives of IT network deployment and service delivery.

Cloud services are based upon five principal characteristics that demonstrate their relation to, and differences from, traditional computing approaches (CSA Security Guidance, 2009). These characteristics are: (i) abstraction of infrastructure, (ii) resource democratization, (iii) service oriented architecture, (iv) elasticity/ dynamism, (v) utility model of consumption and allocation.

Abstraction of infrastructure: The computation, network and storage infrastructure resources are abstracted from the application and information resources as a function of service delivery. Where and by what physical resource that data is processed, transmitted and stored on becomes largely opaque from the perspective of an application or services' ability to deliver it. Infrastructure resources are generally pooled in order to deliver service regardless of the tenancy model employed – shared or dedicated. This abstraction is generally provided by means of high levels of virtualization at the chipset and operating system levels or enabled at the higher levels by heavily customized file systems, operating systems or communication protocols.

Resource democratization: The abstraction of infrastructure yields the notion of resource democratization- whether infrastructure, applications, or information – and provides the capability for pooled resources to be made available and accessible to anyone or anything authorized to utilize them using standardized methods for doing so.

Service-oriented architecture: As the abstraction of infrastructure from application and information yields well-defined and loosely-coupled resource democratization, the notion of utilizing these components in whole or part, alone or with integration, provides a services oriented architecture where resources may be accessed and utilized in a standard way. In this model, the focus is on the delivery of service and not the management of infrastructure.

Elasticity/dynamism: The on-demand model of cloud provisioning coupled with high levels of automation, virtualization, and ubiquitous, reliable and high-speed connectivity provides for the capability to rapidly expand or contract resource allocation to service definition and requirements using a self- service model that scales to as-needed capacity. Since resources are pooled, better utilization and service levels can be achieved.

Utility model of consumption and allocation: The abstracted, democratized, service-oriented and elastic nature of cloud combined with tight automation, orchestration, provisioning and self-service then allows for dynamic allocation of resources based on any number of governing input parameters. Given the visibility at an atomic level, the consumption of resources can then be used to provide a metered utility- cost and usage model. This facilitates greater cost efficacies and scale as well as manageable and predictive costs.

2.1 Cloud Service Delivery Models

Three archetypal models and the derivative combinations thereof generally describe cloud service delivery. The three individual models are often referred to as the “SPI MODEL”, where “SPI” refers to Software, Platform and Infrastructure (as a service) respectively (CSA Security Guidance, 2009).

2.1.1 Software as a Service (SaaS): The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as web browser. In other words, in this model, a complete application is offered to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are services. On the customers’ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. In summary, in this model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Currently, SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho etc.

2.1.2 Platform as a Service (PaaS): In this model, a layer of software or development environment is encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider’s infrastructure. Hence, a capability is provided to the customer to deploy onto the cloud infrastructure customer-created applications using programming languages and tools supported by the provider (e.g., Java, Python, .Net etc.). Although the customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but he/she has the control over the deployed applications and possibly over the application hosting environment configurations. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of operating systems and application servers, such as LAMP (Linux, Apache, MySql and PHP) platform, restricted J2EE, Ruby etc. Some examples of PaaS are: Google's App Engine, Force.com, etc.

2.1.3 Infrastructure as a Service (IaaS): This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers etc.). Some examples of IaaS are: Amazon, GoGrid, 3 Tera etc.

Understanding the relationship and dependencies between these models is critical. IaaS is the foundation of all cloud services with PaaS building upon IaaS, and SaaS-in turn – building upon PaaS. An architecture of cloud layer model is depicted in Figure 1.

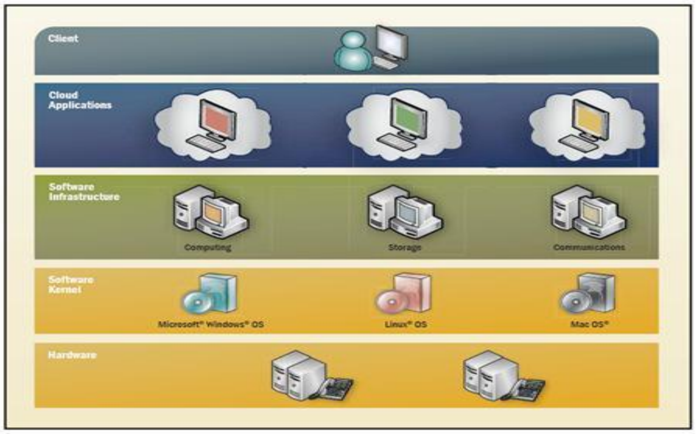


Figure 1: An architecture of the layer model of cloud computing

3. Cloud Service Deployment and Consumption Models

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed (CSA Security Guidance, 2009). Cloud integrators can play a vital role in determining the right cloud path for a specific organization.

Public cloud: Public clouds are provided by a designated service provider and may offer either a single- tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off- premises). All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

Private cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds:

(i) on-premise private clouds and (ii) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider.

Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Managed cloud: Managed clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider.

4 CONCLUSION

This paper has considered number of impacts of cloud computing on digital forensic investigations. It has focused on technical and legal difficulties faced by a forensic investigator during investigation in virtual environment. If we see current scenario of the world, more businesses and organizations will be moving their data to cloud environments in near future. Development in the IT sector will create new complexities for the Crime investigators in accessing, retrieving and acquisition of evidential data. With the emerging technology there will be growth in cybercrime and the demand to conduct forensic investigation on cloud will increase.

Such investigations may face lack of guidance, tools and techniques to retrieve evidence in a forensically sound manner. There is also the need for sound laws regarding clouds including data retention and privacy. Current available laws should be re-examined because of the need to precede ahead and combating criminals.

5 REFERENCES

1. V. Vinaya, P. Sumathi, “Implementation of Effective Third Party Auditing for Data Security in Cloud”,
2. International Journal of Advanced Research in Computer Science and Software Engineering (I.J.A.R.C.S.S.E), Volume 3, Issue 5, May 2013.
3. https://www.ibm.com/developerworks/communiy
4. http://djacademy.ac.in/TechFreaks/cloud.html
5. http://www.cloudstoragecenters.com/advantages-and-disadvantages-of-cloud-computing-system/
6. Casey, E. Handbook of Computer Crime Investigation, Academic Press. Boston. 2002.
7. W. Kruse, J. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley. New York. 2002.
8. R. Richardson, CSI Computer Crime and Security Survey, 2008.
9. http://www.gocsi.com/forms/csi_survey.jhtml (March/April 2009).
10. M.K Rogers, K. Seigfried, “The Future of Computer Forensics: A Needs Analysis.