ISBN No: 978-81-941751-6-2

October, 2019

Paper 18

CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Vaikunth Pai
College of Computer and Information Science,
Srinivas University,
City Campus,
Mangalore-01, India
vpaistar@yahoo.com

Abstract

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

Keywords: Cloud Computing, Scalability, Infrastructure, IT.

Introduction

The advancements in Information Technology (IT) demand a new computing paradigm that supports delivery of computing services on minimal charges without installing them at local sites. Cloud computing offers the same model having above describe properties in which services are delivered over internet in an on-demand elastic way for which the charges are paid at release time of resources. In general, cloud is a multifarious technological paradigm that is an extension of many existing technologies viz. parallel and distributed computing, Service-Oriented-Architecture (SOA), virtualization, networking etc. The distributed computing, virtualization and internet works as indispensable building blocks of the cloud computing. It is a highly sharable computing paradigm where processing, storage, network, applications etc. are shared. The objective of the cloud computing is to provide secure, qualitative, scalable, quick, more responsive, on demand, cost-efficient and automatically provisioned services viz. computation services, storage services, networking etc. being provided in a transparent way (location independent). Cloud computing can help to improve business performance while making a contribution to control the cost of delivering IT resources to any organization.

ISBN No: 978-81-941751-6-2
October, 2019

Architecture of Cloud Computing

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. 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.

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. 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 selfservice model that scales to as-needed capacity. Since resources are pooled, better utilization and service levels can be achieved.

ISBN No: 978-81-941751-6-2
October, 2019

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.

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.

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.

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.

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.,

ISBN No: 978-81-941751-6-2

October, 2019

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.

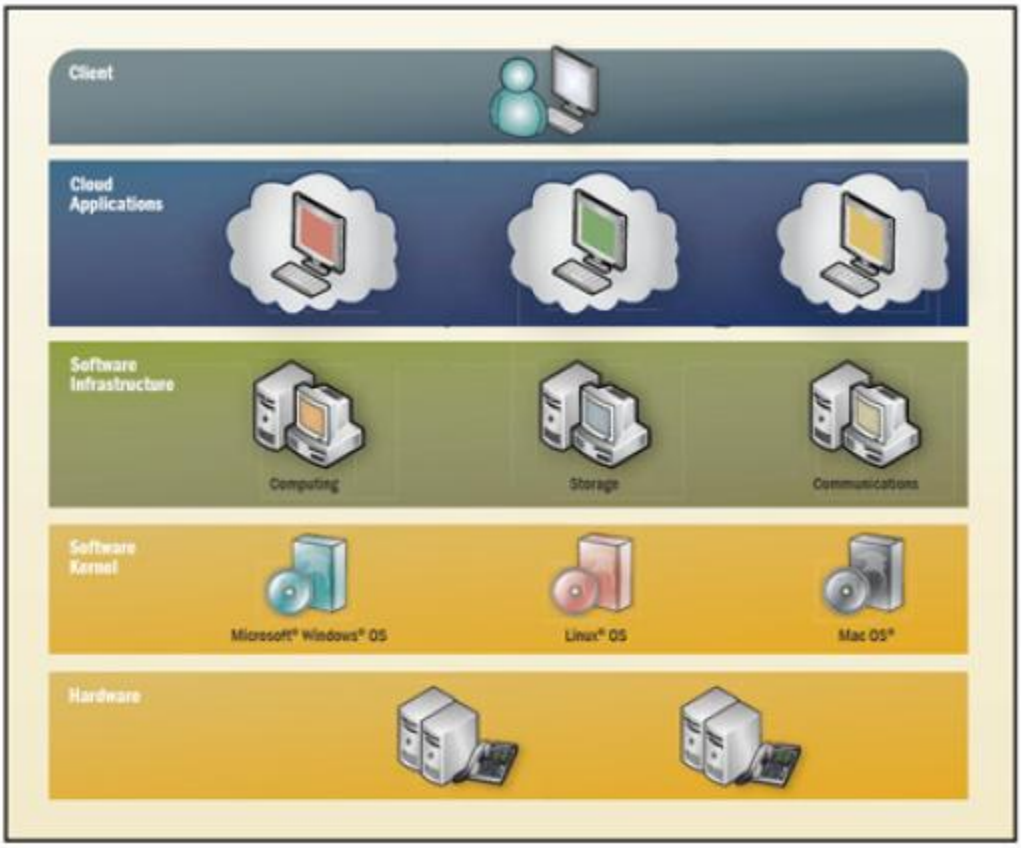

Figure 1: An architecture of the layer model of cloud computing

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 . 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

ISBN No: 978-81-941751-6-2
October, 2019

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.

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.

Issues and Challenges of Cloud Computing

The issues must be addressed in order to provide high quality services to the users while complying with the service provider's needs are security, protection, identity management, resource management, power and energy management, data isolation, availability of resources, heterogeneity of resources.

A. Security and Privacy

According to the survey of International Data Corporation (IDC), Security, Performance and Availability are the three biggest issues in cloud adoption. The critical challenge is how it addresses security and privacy issues which occur due to movement of data and application on networks, loss of control on data, heterogeneous nature of resources and various security policies. Data stored, processing and movement of data outside the controls of an organization poses an inherent risk and making it vulnerable to various attacks. The security threats can be of two types viz. internal and external. The external risk is posed by various persons and organizations e.g. enemies or hackers that do not have direct access to the cloud. The internal
security risk is a well-known issue which can be posed by organizational affiliates, contractors, current or former employees and other parties that have received access to an organization's servers, networks and data to facilitate operations. Cloud computing poses privacy concerns because the service providers may access the data that is on the cloud that

ISBN No: 978-81-941751-6-2

October, 2019

could accidentally or deliberately be changed or even removed posing serious business trust and legal consequences.

B. Performance

According to IDC's survey, performance is the second biggest issue in cloud adoption. The cloud must provide improved performance when a user moves to cloud computing infrastructure. Performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources viz. disk space, limited bandwidth, lower CPU speed, memory, network connections etc. Many times users prefer to use services from more than one cloud where some applications are located on private clouds while some other data or applications being on public and/or community cloud. The data intensive applications are more challenging to provide proper resources. Poor performance can results in end of service delivery, loss of customers, reduce bottom line revenues etc.

C. Reliability and Availability

Any technology's strength is measured by its degree of reliability and availability. Reliability denotes how often resources are available without disruption (loss of data, code reset during execution) and how often they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time. One way to achieve reliability is redundant resource utilization. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned. Regardless of employing architectures having attributes for high reliability and availability, the services in cloud computing can experience denial of service attacks, performance slowdowns, equipment outages and natural disasters. In order to remove FUDD (fear, uncertainty, doubt, and disinformation), probably the reliability, availability and security are the important and prime concern to an organization. Therefore, the level of reliability and availability of cloud resources must be considered as a serious issue into the organization's planning to set up the cloud infrastructure in order to provide effective services to consumers.

D. Scalability and Elasticity

Scalability and elasticity are the most amazing and unique features of the cloud computing. These features provide users to use cloud resources being provisioned as per their need in unlimited amount as required. Scalability can be defined as the ability of the system to perform well even when the resources have been scaled up. Elasticity, on the other hand, is the ability to scale resources both up and down as and when required. Elasticity goes one step further, though, and does also allow the dynamic integration and extraction of physical resources to the infrastructure. The elastic cloud computing means that allocation of resources can get bigger or smaller depending on the requirement. Elasticity enables scalability—which means the system can easily scale up or down the level of services to which the user has subscribed. Scalability can be provided in two ways- horizontally and vertically whereby horizontal scalability (Scale Out) refers to addition of more nodes to the system such as adding a new computer to an existing service provider system while vertical scalability (scale up) refers to addition of resources to a single node in the system, typically involving the addition of memory or processors to a single computer.

ISBN No: 978-81-941751-6-2

October, 2019

E. Interoperability and Portability

Interoperability is the ability to use the same tools or application across various cloud service providers platforms. The interoperability can be defined at various levels viz. application, service, management and Data interoperability. Cloud users must have the flexibility of migrating in and out and switching to clouds whenever they want without no vendor lock-in period. One of the adoption barriers in cloud computing interoperability is the vendor lock-in risk. The main problems to realize it are the lack of open standards, open APIs and lack of standard interfaces for VM formats and service deployment interfaces. Cloud portability ensures that one cloud solution will be able to work with other platforms and applications as well as with other clouds.

F. Resource Management and Scheduling

Resources management can be consider at various levels viz. hardware, software, virtualization level with performance, security and other parameters being dependent on the management and provisioning of resources. It includes the management of memory, disk space, CPU's, cores, threads, VM images, I/O devices etc. Resource provisioning can be defined as allocation and management of resources to provide desired level of services. Job scheduling is a type of resource provisioning where jobs execution order is established in order to finish job execution to optimize some parameters viz. turnaround time, response time, waiting time, throughput and resource utilization. Since cloud computing is a combination of many existing technologies, existing job scheduling strategies are eligible to be applied on cloud system. The major issues of job scheduling on cloud systems are partitioning of jobs into parallel tasks, interconnection network between clouds or processors, assigning priority to jobs and selection of processors or cloud to allocate the job(s), job flexibility, level of pre-emption supported, workload characteristics, memory allocation, task execution monitoring, recourse allocation requirements, topology, nature of the job, effect of existing load, load balancing, parallelism, job migration policy, redundant Resource selection, synchronization, communication overheads, job pre processing requirements etc. The job scheduling is one of critical process that must be decided very carefully and wrong selection of scheduling strategy can lead to devastating effect on performance leading to wastage of resources while falling to meet Quality of Service (QoS) standards.

G. Energy Consumption

Cloud data centers house thousands of servers and set up the cooling infrastructure to remove heats generated by these servers. These servers and cooling infrastructure consume a large amount of energy and produces green house gases (GHGs). In addition, the cloud data centres which are inherent part of the cloud infrastructure are also very expensive to operate and consume energy at a very large scale. For example, the power consumption of Google data centre is equivalent to a city such as San Francisco. Since ICT aids towards developing applications and facilities for human prosperity, we require designing such hardware, software, scheduling policies, networks and other protocols that consume energy in ecofriendly and optimized manner. The goal is not only to reduce the consumption of energy and hence the cost consumed by data centers, but also to maintain environmental standards necessary not only to survive but to thrive.

ISBN No: 978-81-941751-6-2

October, 2019

H. Bandwidth Cost

High speed communication channels work as a backbone of cloud computing. With cloud computing, business gets the ability to save money on hardware and/or software but still requires spending more on the bandwidth. It is almost impossible to fully exploit the services of cloud computing without high speed communication channels. Migration to cloud almost removes the up-front cost, while it increases the cost of data communication on network i.e. the cost involved in transfer of data to and from the private and other clouds. This problem is prominent if consumer application is data intensive and the consumer's data is distributed amongst a number of clouds (private/public/community).

Conclusion

Cloud computing can be considered as an integral component of almost all businesses in near future and it is expected to change the landscape of IT industry. It is based on the model of delivering services on internet with pay-as-you-go model with advantages like no up-front cost, lower IT staff, lower cost of operation to name a few. Although cloud computing has bright prospects both for business and researchers certain challenging issues including security, performance, reliability, scalability, interoperability, virtualization etc. needs to be addressed carefully. The improvement in bandwidth technology, corresponding service models and security models can really revolutionize this area along with the IT industry. The paper has discussed the concept of cloud computing and shades some lights on various issues and challenges that needs to be addressed in order to realize the implementation of the cloud and making it a dominant part of our life in order to thrive.