

Cloud Computing: Security Issues and Research Challenges

Aniket A. Sakpal
MET Institute of Computer Science

ABSTRACT

Cloud computing is architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

Keywords: *Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing*

1. INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers. Cloud computing appeared as a business necessity, being animated by the idea of just using the infrastructure without managing it. Although initially this idea was present only in the academic area, recently, it was transposed into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs.

Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser.

2. CLOUD COMPUTING BUILDING BLOCKS

2.1 Different models of cloud computing

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software-as-a-Service (SaaS): SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

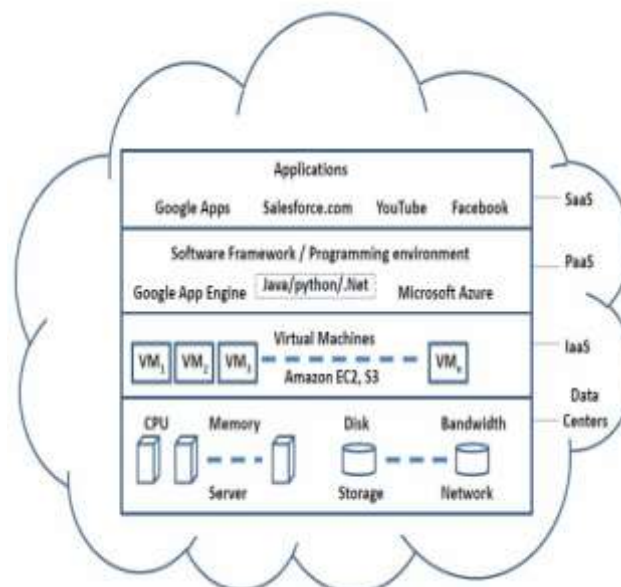


Figure 1: High Level View of Cloud Computing Architecture

Platform as a Service (PaaS): “PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. An example of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, and GoGrid.

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.

Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure 1.

2.2 Cloud computing entities

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows

Cloud Providers: Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers.

Cloud Service Brokers: Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

Cloud Resellers: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed.

3. CLOUD COMPUTING SECURITY ARCHITECTURE

Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service. Users will not compromise their privacy so cloud computing service providers must ensure that the customers' information is safe. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information. Some of the important components of Service Provider Layer are SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler & Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and Binding Issues. Some of the important components of Virtual Machine Layer create number of virtual machines and number of operating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management. Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and storage, and is henceforth typically denoted as Infrastructure-as-a-Service (IaaS). Some of the security issues related to Data Center Layer are secure data at rest, Physical Security: Network and Server.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues. They propose the OSA pattern, which pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis. For example, the Certification, Accreditation, and Security Assessments series increase in importance to ensure oversight and assurance given that the operations are being "outsourced" to another provider. System and Services Acquisition is crucial to ensure that acquisition of services is managed correctly. Contingency planning helps to ensure a clear understanding of how to respond in the event of interruptions to service delivery. The Risk Assessment controls are important to understand the risks associated with services in a business context. National Institute of Standard and Technology (NIST), USA (<http://www.nist.gov/>) has initiated activities to promote standards for cloud computing. To address the challenges and to enable cloud computing, several standards groups and industry consortia are developing

4. ACKNOWLEDGMENT

This research was supported/partially supported by Omprakash Mandge. We thank our colleagues from who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

We are also immensely grateful to all those who supported us and for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

5. REFERENCES

- [1] <https://computer.howstuffworks.com/cloud-computing/cloud-computing3.htm>
- [2] https://en.wikipedia.org/wiki/Cloud_computing
- [3] http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
- [4] <http://in.pcmag.com/networking-communications-software/38970/feature/what-is-cloud-computing>