Security Issues in Cloud Computing: A Critical Analysis

[1]Dr. G. Manoj Someswar, [2]K. Vidya Shekar
[1]Anwar-ul-Uloom College of Engineering & Technology, Vikarabad, AP, India
[2]System Analyst, Sagar Soft India Cyber Towers, Hitech City, Madhapur, Hyderabad, AP, India

Abstract
Cloud computing refers to applications and services that run on a distributed network using virtualized resources and accessed by common Internet protocols and networking standards. Cloud computing represents a paradigm shift driven by the increasing demand of Web based applications for elastic, scalable and efficient system architectures that can efficiently support their ever-growing data volume and large-scale data analysis. When it comes to Security, cloud really suffers a lot. The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud.

Keywords
Cloud Computing, Scalability, Security, Infrastructure

I. Introduction

Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be deployed by the vendor, and used by the client. It also shares necessary software's and on-demand tools for various IT Industries. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [1]. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [2-3].

A. Definition

A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service). Amazon is the first company to look into the growing importance of Cloud computing very seriously followed by Google and IBM. Some of the other companies which make use of Cloud are Salesforce.com, Zoho, Rackspace, Microsoft.

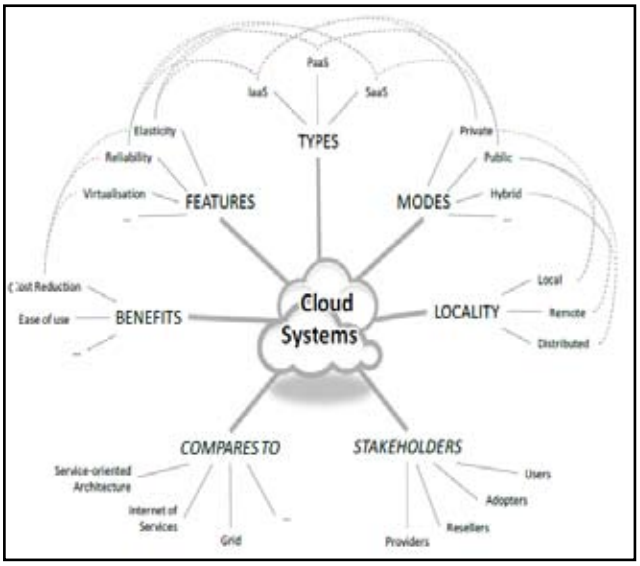

Fig. 1: Cloud

Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises [4].

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to Cloud it's more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud.

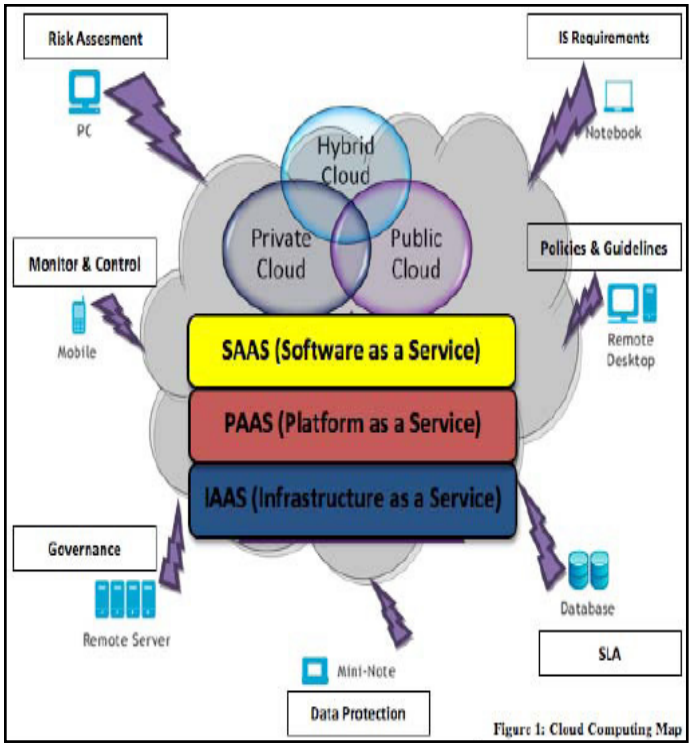

Fig 2: Cloud Deployment Model

II. Scientific and Technologic Context

A. Types of Clouds

Cloud providers typically centre on one type of cloud functionality provisioning: Infrastructure, Platform or Software / Application, though there is potentially no restriction to offer multiple types at the same time, which can often be observed in PaaS (Platform as a Service) providers which offer specific applications too, such as Google App Engine in combination with Google Docs.

The following list identifies the main types of clouds (currently in use):

Infrastructure as a Service (IaaS) also referred to as Resource Clouds, provide (managed and scalable) resources as services to the user – in other words, they basically provide enhanced virtualisation capabilities. Accordingly, different resources may be provided via a service interface.

Data & Storage Clouds deal with reliable access to data of potentially dynamic size, weighing resource usage with access requirements and / or quality definition.

1. Examples: Amazon S3, SQL Azure

Compute Clouds provide access to computational resources, i.e. CPUs. So far, such low-level resources cannot really be exploited on their own, so that they are typically exposed as part of a "virtualized environment" (not to be mixed with PaaS below), i.e. hypervisors. Compute Cloud Providers therefore typically offer the capability to provide computing resources (i.e. raw access to resources unlike PaaS that offer full software stacks to develop and build applications), typically virtualised, in which to execute cloudified services and applications. IaaS (Infrastructure as a Service) offers additional capabilities over a simple compute service.

2. Examples: Amazon EC2, Zimory, Elastichosts

Platform as a Service (PaaS), provide computational resources via a platform upon which applications and services can be developed and hosted. PaaS typically makes use of dedicated APIs to control the behaviour of a server hosting engine which executes and replicates the execution according to user requests (e.g. access rate). As each provider exposes his / her own API according to the respective key capabilities, applications developed for one specific cloud provider cannot be moved to another cloud host – there are however attempts to extend generic programming models with cloud capabilities (such as MS Azure).

3. Examples: Force.com, Google App Engine, Windows Azure (Platform)

Software as a Service (SaaS), also sometimes referred to as Service or Application Clouds are offering implementations of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications / services using a cloud infrastructure or platform, rather than providing cloud features themselves. Often, kind of standard application software functionality is offered within a cloud.

4. Examples: Google Docs, Salesforce CRM, SAP Business by Design

Overall, Cloud Computing is not restricted to Infrastructure / Platform / Software as a Service systems, even though it provides enhanced capabilities which act as (vertical) enablers to these systems. As such, I/P/SaaS can be considered specific "usage patterns" for cloud systems which relate to models already approached by Grid, Web Services etc. Cloud systems are a promising way to implement these models and extend them further.

B. Deployment Types (Cloud Usage)

Similar to P/I/SaaS, clouds may be hosted and employed in different fashions, depending on the use case, respectively the business model of the provider. So far, there has been a tendency of clouds to evolve from private, internal solutions (private clouds) to manage the local infrastructure and the amount of requests e.g. to ensure availability of highly requested data. This is due to the fact that data centres initiating cloud capabilities made use of these features for internal purposes before considering selling the capabilities publicly (public clouds). Only now that the providers have gained confidence in publication and exposition of cloud features do the first hybrid solutions emerge. This movement from private via public to combined solutions is often considered a "natural" evolution of such systems, though there is no reason for providers to not start up with hybrid solutions, once the necessary technologies have reached a mature enough position.

We can hence distinguish between the following deployment types:

Private Clouds are typically owned by the respective enterprise and / or leased. Functionalities are not directly exposed to the customer, though in some cases services with cloud enhanced features may be offered – this is similar to (Cloud) Software as a Service from the customer point of view.

1. Example: eBay

(i). Public Clouds

Enterprises may use cloud functionality from others, respectively offer their own services to users outside of the company. Providing the user with the actual capability to exploit the cloud features for his / her own purposes also allows other enterprises to outsource their services to such cloud providers, thus reducing costs and effort to build up their own infrastructure. As noted in the context of cloud types, the scope of functionalities thereby may differ.

2. Example: Amazon, Google Apps, Windows Azure

(i). Hybrid Clouds

Though public clouds allow enterprises to outsource parts of their infrastructure to cloud providers, they at the same time would lose control over the resources and the distribution /management of code and data. In some cases, this is not desired by the respective enterprise. Hybrid clouds consist of a mixed employment of private and public cloud infrastructures so as to achieve a maximum of cost reduction through outsourcing whilst maintaining the desired degree of control over e.g. sensitive data by employing local private clouds. There are not many hybrid clouds actually in use today, though initial initiatives such as the one by IBM and Juniper already introduce base technologies for their realization .

(ii). Community Clouds

Typically cloud systems are restricted to the local infrastructure, i.e. providers of public clouds offer their own infrastructure to customers. Though the provider could actually resell the infrastructure of another provider, clouds do not aggregate infrastructures to build up larger, cross-boundary structures. In particular smaller SMEs could profit from community clouds to which different entities contribute with their respective (smaller) infrastructure. Community clouds can either aggregate public clouds or dedicated resource infrastructures.

(iii). Special Purpose Clouds

In particular IaaS clouds originating from data centres have a "general purpose" appeal to them, as their according capabilities can be equally used for a wide scope of use cases and customer types. As opposed to this, PaaS clouds tend to provide functionalities more specialized to specific use cases, which should not be confused with "proprietariness" of the platform: specialization implies providing additional, use case specific methods, whilst proprietary data implies that structure of data and interface are specific to the provider. Specialized functionalities are provided e.g. by the Google App Engine which provides specific capabilities dedicated to distributed document management. Similar to general service provisioning (web based or not), it can be expected that

future systems will provide even more specialized capabilities to attract individual user areas, due to competition, customer demand and available expertise. Special Purpose Clouds are just extensions of "normal" cloud systems to provide additional, dedicated capabilities. The basis of such development is already visible.

C. Cloud Environment Roles

In cloud environments, individual roles can be identified similar to the typical role distribution in Service Oriented Architectures and in particular in (business oriented) Virtual Organisations. As the roles relate strongly to the individual business models it is imperative to have a clear definition of the types of roles involved in order to ensure common understanding.

1. (Cloud) Providers

Offer clouds to the customer – either via dedicated APIs (PaaS), virtual machines and / or direct access to the resources (IaaS). Note that hosts of cloud enhanced services (SaaS) are typically referred to as Service Providers, though there may be ambiguity between the terms Service Provider and Cloud Provider.

2. (Cloud) Resellers or Aggregators

Aggregate cloud platforms from cloud providers to either provide a larger resource infrastructure to their customers or to provide enhanced features (see II.B). This relates to community clouds in so far as the cloud aggregators may expose a single interface to a merged cloud infrastructure. They will match the economic benefits of global cloud infrastructures with the understanding of local customer needs by providing highly customized, enhanced offerings to local companies (especially SME's) and world-class applications in important European industry sectors. Similar to the software and consulting industry, the creation of European cloud partner ecosystems will provide significant economic opportunities in the application domain – first, by mapping emerging industry requests into innovative solutions and second by utilizing these innovative solutions by European companies in the global marketplace.

3. (Cloud) Adopters or (Software / Services)

Vendors enhance their own services and capabilities by exploiting cloud platforms from cloud providers or cloud resellers. This enables them to e.g. provide services that scale to dynamic demands – in particular new business entries who cannot estimate the uptake / demand of their services. The cloud enhanced services thus effectively become software as a service.

4. (Cloud) Consumers or Users

Make direct use of the cloud capabilities – as opposed to cloud resellers and cloud adopters, however, not to improve the services and capabilities they offer, but to make use of the direct results, i.e. either to execute complex computations or to host a flexible data set. Note that this involves in particular larger enterprises which outsource their inhouse infrastructure to reduce cost and efforts. Note that future market developments will most likely enable the user to become provider and consumer at the same time, thus following the "Prosumer" concept, as already introduced by the Service Oriented Architecture concepts.

5. (Cloud) Tool Providers

Do not actually provide cloud capabilities, but supporting tools such as programming environments, virtual machine management.

III. Project Objective

The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy.

A. Security Issues Faced by Cloud Computing

1. Data Integrity
2. Data Theft
3. Privacy issues
4. Infected Application
5. Data loss
6. Data Location
7. Security on Vendor level
8. Security on user level

B. Protecting the Cloud

A Secure cloud is always a reliable source of information thus protecting the cloud is a very important task for security professionals who are in charge of the cloud.

Consider a proxy/broker service.Some of the ways by which a cloud can be protected are Protection of data, making sure data is available for the customers, delivering high performance for the Customers, using Intrusion Detection System on Cloud to monitor any malicious activities, to make sure the application used by the customer is safe to use, Vendors must provide a support system for the customer, customer should be able to recover any loss of data in the cloud.

Most important of them all is that, there should be a good degree of encryption provided by the vendor to the customer that only the customer should be able to access the data and not the malicious User.

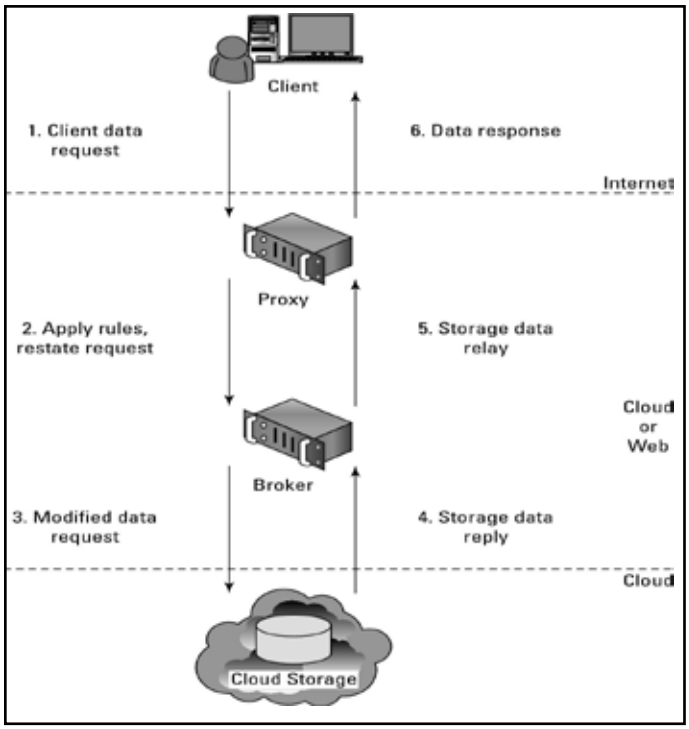

Fig 3: Cloud Storage

C. Cloud Computing Challenges

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

1. Security

It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines)
pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack

2. Costing Model

Cloud consumers must consider the tradeoffs amongst computation,communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs.

3. Charging Model

The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and redeve lopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud
providers.

4. Service Level Agreement (SLA)

Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.

IV. Conclusion

Both the Vendor and the customer should make sure that the cloud is safe from all the external threats, thus there will be a mutual understanding between the customer and the vendor when it comes to the security on Cloud.

References

[1] Harjit Singh Lamba, Gurdev Singh,"Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, Vol. 2, No. 3, Department of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.
[2] Dr. Gurdev Singh, Shanu Sood, Amit Sharma,"CM-Measurement Facets for Cloud Performance", IJCA, Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Vol. 23, No. 3, June 2011.
[3] Joachim Schaper,"Cloud Services", 4th IEEE International Conference on DEST, Germany, 2010.
[4] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packets ormsecurity.net/.../ ProblemsFacedbyCloudComputing.pdf.

Dr.G.Manoj Someswar, B.Tech., M.S. (USA), M.C.A., Ph.D. is having 20+ years of relevant work experience in Academics, Teaching, Industry, Research and Software Development. At present, he is working as PRINCIPAL Anwarul-uloom College of Engineering & Technology Yennepally, Vikarabad - 501101, RR Dist., AP, and utilizing his teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. He has attended more than 100 national and international conferences, seminars and workshops. He has more than 10 publications to his credit both in national and international journals. He is also having to his credit more than 50 research articles and paper presentations which are accepted in national and international conference proceedings both in India and Abroad.

K.Vidya Shekar M.tech, Working as Software Engineer at SAGAR SOFT, Hyderabad. He Previously worked as Assistant Professor in CSE Department at Srinidhi Institute of Science and Technology, Hyderabad,A.P. He is having 7 years of Teaching Experience.