Security Aspects of Cloud Computing

G.N.K.Suresh Babu¹ S.K.Saravanan² and Dr.S.K.Srivatsa³

¹Associate Professor, Department of Computer Applications, GKMCE, Chennai.
²Assistant Professor[SG], Department of Computer Applications, Valliammai Engineering College, Chennai.
³Sr.Professor – St.Joseph’s College of Engineering, Chennai.

ABSTRACT
The goal of this article is to identify the main security issues and to draw the attention of both decision makers and users to the potential risks of moving data into the cloud. Cloud computing is one of the latest developments in the computer field also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. Cloud computing is model which uses combine concept of “software-as-a-service” and “utility computing”, provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so 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, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. This paper first discusses the overview of cloud computing and what are all the security issues it faces and finally it gives the proposed solutions also.

Keywords: IaaS, PaaS, SaaS, Security, Storage

1. Introduction

Cloud computing is one of the most significant transformation in information technology with many advantages to both companies and end users. This technology promises to release the
client from the burden of administering more and more complex and expensive systems by offering him the possibility of using systems with state of art computing capabilities, high availability and scalability. Given the theorists’, network architects’, developers’, managers’, consumers’, etc. constant scrutiny over this subject, there is a plethora of definitions that attempt to address the concept of cloud computing. Therefore, this article will use a generic definition which, even if not a comprehensive one, it will include the most important dimensions and variables. Thus, cloud computing is a model of organizing computers for enabling convenient, ubiquitous, on demand network access to a shared pool of configurable IT resources. Cloud computing has the potential to enhance collaboration, agility, scaling and availability and provides opportunities for cost reduction through optimized and efficient use of computing resources. The cloud model is a way of organizing computers so that resources can be quickly orchestrated, provisioned, implemented and decommissioned, scaled up or down to provide an on demand service allocation.

2. Cloud Computing Architecture

In this paragraph the different service models of cloud computing are distilled. There are three different levels of services models. It starts from the lowest service model which is called Infrastructure As A Service (IAAS) and builds up via Platform As A Service (PAAS) to Software As A Service (SAAS). Each level adds extra functionality and abstraction of the technical details of the services which are offered.
As shown in Figure 1 the different levels provide their services to different types of users from network engineers to end users.

2.1 IaaS

Infrastructure as a Service (IaaS): is the lowest layer where users use computing resources such as databases, CPU power, memory and storage from an IaaS provider and use the resources to deploy and run their applications. In contrast to the PaaS model, the IaaS model allows users to access the underlying infrastructure through the use of virtual machines which automatically can scale up and down. IaaS gives users more flexibility than PaaS as it allows the user to deploy any software stack on top of the operating system. However, this flexibility comes with a cost and users are responsible for updating and patching the operating system at the IaaS level. Amazon Web Services’ EC2 and S3 are popular IaaS examples.
2.2 PAAS

Platform as a Service (PaaS): is the layer where applications are developed using a set of programming languages and tools that are supported and provided by the PaaS provider. PaaS provides developers with a high level of abstraction that allows them to focus on developing their applications. Developers can provide their customers with a custom developed application without the hassle of defining and maintaining the infrastructure. Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine and Microsoft Azure are popular PaaS examples.

2.3 SAAS

Software as a Service (SaaS): is a cloud computing layer where users simply make use of a web-browser to access software that others have developed, maintain and offer as a service over the web. At the SaaS level, users do not have control or access to the underlying platform and infrastructure that is being used to host the software. Sales force’s Customer Relationship Management and Google gmail are popular examples that use the SaaS model of cloud computing.

3 Cloud Computing Deployment Model

The three different service models can be deployed for a customer in various ways varying from the public internet to a private data center.

3.1 Public

Public is a deployment strategy which uses the publicly available internet to deliver the services to the users. A great advantage of this deployment type is that the services are available from any internet connection, an down side however is the security. The cloud services like Gmail and Azure are services provided trough the public cloud.
3.2 Private

This deployment strategy can be compared with the traditional in-house hosting of a service, however it uses the technologies on which cloud computing is based such as virtualization to provide advantages to the organization.

3.3 Community

A community cloud is a bit like a private cloud however the cloud is shared among a community of organizations. This is done to divide the costs and risks of running a own cloud. These clouds can be found in shared service centers which service multiple organizations.

3.4 Hybrid

A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon's Elastic Compute Cloud (EC2) for general computing but store customer data within its own data center.

4. Essential Characteristics of Cloud Computing

As described above, there are 5 essential characteristics of Cloud Computing which explains there relation and difference from the traditional computing.

- On-demand-self-service
  Consumer can provision or un-provision the services when needed, without the human interaction with the service provider.

- Broad Network Access
  It has capabilities over the network and accessed through standard mechanism.

- Resources Pooling
The computing resources of the provider are pooled to serve multiple consumers which are using a multi-tenant model, with various physical and virtual resources dynamically assigned, depending on consumer demand.

- Rapid Elasticity
  Services can be rapidly and elastically provisioned.

- Measured Service
  Cloud Computing systems automatically control and optimize resource usage by providing a metering capability to the type of services (e.g. storage, processing, bandwidth, or active user accounts)

5. Pros and Cons of Cloud Computing

5.1 Pros of cloud computing

Cloud computing has a number of advantages, many of them economically beneficial to both large companies and individual users.

- No need for an expensive, high-power computer
- No need to fill your hard drive with programs
- Many programs stored on the cloud are free to use
- Virtually unlimited storage
- Access to documents virtually anywhere

It can be an economical option for a number of users, from businesses to individuals. Because the programs are stored on a remote server, users don’t require expensive powerful computers or need to spend hundreds of dollars on individual programs. Cloud lets you have free access to many useful programs.

5.2 Cons of cloud computing
There are a number of conditions and risks associated with cloud that potential users may want to consider.

- It requires a fast, continual Internet connection
- The connection can be slow if many users are accessing the server
- Information may not be secure
- Programs on the server may not be the full version.

Because a large number of people may be attempting to access a remote server at one time, the cloud connection can be slow. It can also be less secure than on-site computing since so many individuals are given access to the server. Even though many of the programs offered on cloud are free to access, they may not be the full versions. Using cloud is an economical option for both businesses and individuals. It can provide low cost access to a number of useful programs and almost unlimited storage space. But the platform is also not as secure as an on-site server that can create security issues. Consider these pros and cons when deciding whether to utilize cloud computing benefits.


Two main issues exist with security and privacy aspects of Cloud Computing:

1. loss of control over data and
2. dependence on the Cloud Computing provider.

These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.

Typical issues due to the loss of control over data are:
1. Most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. Data could be compromised by the Cloud Computing provider itself or other competitive enterprises which are customers with the same Cloud Computing provider. There is a lack of transparency for customers on how, when, why and where their data is processed. This is in opposition to the data protection requirement that customers know what happens with their data.

2. Many Cloud Computing providers are technically able to perform data mining techniques to analyse user data. This is a very sensitive function and even more so, as users are often storing and processing sensitive data when using Cloud Computing services. This holds especially true for social media applications that encourage users to share much of their private life e.g. private photos.

3. Mobile devices, in particular with their limited storage and computing capabilities are drivers for having services provided by Cloud Computing instead of using software on individual computers. Even data that are only to be transferred from one mobile device to another (local) device, are often transferred via the cloud, when cloud oriented applications on the mobile devices are involved. Therefore users often put themselves at risk without noticing this, as they assume that the data is transferred locally.

4. Since Cloud Computing is a service, it has to be accessed remotely. The connection between the Cloud Computing provider and customer is not always adequately protected. Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.
5. Concerns also exist with regard to deletion of data: It is difficult to delete all copies of electronic material because it is difficult to find all copies. It is impossible to guarantee complete deletion of all copies of data. Therefore it is difficult to enforce mandatory deletion of data. However, mandatory deletion of data should be included into any forthcoming regulation of Cloud Computing services, but still it should not be relied on too much: the age of a “Guaranteed complete deletion of data”, if it ever existed has passed. This needs to be considered, when data are gathered and stored.

6. Data Protection and Privacy legislation is not even similar in many countries around the globe yet Cloud Computing is a global service of the future. Consequently the problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.

7. Cloud computing depends on a reliable and secure telecommunications network that assures and guarantees the operations of the terminal users of the services provided in the cloud by the cloud computing provider. Telecommunications networks are often provided separately from the Cloud computing services.

Typical issues with regard to the dependence on the Cloud Computing provider are:

1. A major concern regarding dependence on a specific Cloud Computing provider is availability. If the Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity.
2. Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider. Therefore a customer does not have anything to refer to if incidents occur or any problems arise.

3. Cloud Computing is a service similar to other more “traditional” services and utilities (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) Both Cloud Computing services and traditional services and utilities tend to be offered by large providers dealing with smaller customers. Therefore the customers usually depend on the providers because it is difficult to change providers if it is possible at all. Consequently traditional services (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) are usually regulated with regard to the functionality range (e.g. mandatory functions, coverage), pricing, liability of the provider, and reliability.

Cloud Computing corroborates a trend that ICT security is no longer a purely technical issue but an issue between individuals and organisations and thus includes both human and organisational aspects such as management, contracting, and legal enforcement.

7. Proposed Solutions

In particular the following points need to be considered.

1. Risk management and (legal) compliance issues must be well defined in the contract between Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data, e.g. the physical location of data storage. In this way the trust between the Cloud Computing provider and customer can be strengthened.

2. The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation.
3. The problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.

4. The Cloud Computing providers should be obliged to ensure data confidentiality.

5. Mandatory deletion of data should be included into potential regulation of Cloud Computing services, but it should not be relied upon too much.

6. The fact that there is no guaranteed complete deletion of data needs to be considered, when data are gathered and stored.

7. In order to guarantee the availability of data, local backup of essential data by customers should be considered.

8. Development and better promotion of software that enables local data transfers between devices should be encouraged.

9. The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks.

10. Adequate logging and auditing should be provided. An external audit can be beneficial for the reputation of the Cloud Computing providers as well as for strengthening the trust with the customer.

8. Security benefits of cloud computing

Cloud Computing has a lot of potential to improve security for enterprises and the ways it can improve security is described below.

Benefits of Scale

It is a fact that all types of security measures which are implemented on a larger scale are cheaper. Hence by adopting Cloud Computing enterprises gets better protection with same amount of money. The security includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances, human resources and their management.
and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Along with these benefits, other benefits include:

**Multiple Locations**

The cloud providers by default have economic resources to replicate content and this increases the redundancy and independence from failure. Hence, it provides the disaster recovery.

**Edge Networks**

Cloud Computing provides reliability, quality increase and less local network problems for enterprises by having storage, processing and delivery closer to the network edge.

**Improved Timelines of Response (incidents)**

Cloud providers have larger to incidents or well-run-larger-scale systems. These systems help in improved timelines of response e.g. because of the early detection of new malware deployments, it can develop more effective and efficient incident response.

**Threat Management**

The small enterprises don’t have resources to hire specialists for dealing with specific security issues but cloud providers can do that and provide better threat management.

**9. Conclusion and Future Work**

Cloud Computing offers better computing through improved utilization and reduced administration and infrastructure costs. Cloud Computing is better for medium and small sized enterprises as compared to large enterprises in terms of both cost and data security. Cloud computing is latest development that provides easy access to high performance computing
resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. Developing countries like India can take the benefits of cloud computing by implementing it in its e-government projects. The paper addresses the issues that can arise during the deployment of cloud services. After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems. Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity, data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown killer application will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in future.

References


July 2013, Volume: 1 Issue: 7


