SECURITY ISSUES IN CLOUD COMPUTING

Mahesh Arun Sale*

Abstract

More and more businesses are seeking cloud services as cloud computing increases its presence in public sector. These cloud services include SaaS (Software as a Service), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) etc. The security nuances of cloud are becoming more evident as cloud computing expands rapidly. Also as more and more information is being put on the cloud, the different cloud security issues are arising. This paper discusses security challenges in cloud computing, security issues regarding Information security, data security, network security, access management etc. Some security practices to be considered for cloud environment are also recommended.

Keywords: Cloud Computing, Encryption, Security, Trust, Vulnerability.

* Assistant Professor, Department of Computer Engineering, College of Engineering, Kopargaon, Maharashtra, India.

Introduction

The concepts of virtualization and cloud computing are breaking the physical bonds between an IT infrastructure and a user which helps companies accomplish more. But the companies must overcome the heightened security threats in order to benefit fully from this new computing paradigm. This can be true for SaaS providers. Also some security concerns are worth to be discussed. For example, in the cloud, you lose control over assets in some respects, so your security model must be reassessed. Enterprise security is only as good as the least reliable partner, department, or vendor. Can you trust your data to your service provider? This paper discusses some issues you should consider before answering that question.

1. Obstacles And Opportunities In Cloud Computing

This section gives a list of obstacles which can occur during the growth of Cloud Computing. Along with the obstacles some opportunities are also given to overcome the obstacles.

1.1 Software Licensing

Software licenses impose restriction on the computers on which the software can run. Customers pay for purchasing software and then pay for its annual maintenance fees. Hence, many Cloud Service Providers has to rely on open source software partly because the licenses for commercial software are not a good match to utility computing.

The opportunity here is that either the open source softwares remain popular or the commercial software companies should take a step to change their licensing structure to better fit Cloud Computing. For example, Microsoft and Amazon now offer pay-as-you-go software licensing for Windows Server and Windows SQL Server on EC2. An EC2 instance running Microsoft Windows costs $0.15 per hour instead of the traditional $0.10 per hour of the open source version [14].

1.2 Service Availability

The users of Cloud Computing always worry about the availability of services from Cloud Service Provider. Most of the SaaS provides have set a high standard in this regard. One of the best examples is Google search engine. If people went to Google to search and it won't be available, they would think the Internet was down. The cloud users expect such availability of service from Cloud Service Provider, which is hard to achieve.

It has been seen that many cloud computing service providers suffer major outages over the past few months. This could impact smaller organizations as they plan to move forward with cloud computing. Some of the major cloud computing service outages in 2011 are in given in [16] including the outages of Amazon Web Services, Gmail and Google Apps.

1.3 Reputation Fate Sharing

Some customers degraded reputation in cloud environment can affect the reputation of cloud as a whole. For example, spam prevention and detection systems can put some IP addresses in blacklist, and thus may limit which applications are hosted in that cloud environment.

1.4 Data Lock-In

Most of the APIs for Cloud Computing are still proprietary, or at least have not been standardized. Thus, the cloud users are unable to extract their data and programs from one site to run on another. This concern of difficulty of extracting data from cloud is preventing organizations from adopting Cloud Computing. Such lock-in of customers may be attractive to Cloud Providers, but then cloud users becomes more vulnerable to price increases, reliability issues etc.

In order to overcome the above problem an obvious solution is standardize the APIs to enable the SaaS developers to deploy services and data across different Cloud Providers. This will ensure that the failure of one Cloud Provider would not take all copies of customer data with it.

1.5 Bottlenecks in Data Transfer

Applications are becoming more data-intensive. If applications are placed across the boundaries of the cloud, this may arise the issues of data placement and transfer. The costs of few hundred per terabytes transferred makes data transfer costs an important issue. Thus cloud providers and users have to think about the implications of data transfer and traffic at every level of cloud system in order to minimize the costs.

One solution to avoid the high cost of data transfer over Internet is to ship the entire disks. Jim Gray [15] found that the cheapest way to transfer a huge data is to physically send disks or even whole computers via overnight delivery services. He experienced only a single failure in 400 attempts.

1.6 Confidentiality and Auditability of Data

No one wants that their sensitive data would get available publicly. Cloud environments are mostly public (rather than private), thus exposing the system to more attacks. It is trivial to secure a cloud computing environment as secure as an in-house IT environment. Most of the problems can be solved immediately with well-known technologies like firewalls, packet filters, encrypted storage, Virtual Local Area Networks, etc. For example, encrypting the customer's data before moving to the cloud will make the data more secure than the unencrypted data in local data centres. Similarly, an additional layer of auditability could be added beyond the reach of the virtualized applications.

1.7 Bugs in Large-Scale Distributed Systems

Removing bugs in large scale distributed systems is one of the difficult challenges in cloud computing. It is normally seen that these bugs cannot be reproduced in smaller configurations, so that the debugging must be done in the production data-centres.

2. Security Challenges In Cloud Computing

In order to provide secure cloud environment we must first understand the security challenges in cloud computing world. Some of the security challenges are listed and discussed below:

2.1 Losing the Control over Data and Physical Infrastructure

Control is an important issue in cloud computing. If we don't have much control over our data, we trust that system less. For example, when we want to withdraw money from ATM we trust the ATM because we get the money. But the trust will be less when there is issue of depositing the money through ATM. Because we don't know what will happen to our money after depositing.

In cloud computing once the data of a cloud user leave its perimeter; the user doesn't have much control over the data or the processes that manipulate them. It doesn't know who can access the data-which is stored on various disks in multiple locations and possibly managed by third-party providers. This lack of control over the data and processes arise the risk of losing data confidentiality, integrity and availability. In cloud computing consumers are required to relinquish control of running their applications and storing their data.

In a public cloud environment the computing resources are shared between different cloud users. In such a shared environment, cloud users don't have any knowledge or control of where the resources run.

2.2 Establishing Trust in Remote Execution Environment

How can cloud providers earn their customers' trust when a third party is processing sensitive data in a remote machine located in various countries?

The problem of trusting a cloud environment is of main concern today. From a user's perspective, computing in the cloud is a loss of control. Why should I trust my computing to the cloud, and to those who run it? Are they trustworthy? Wikileaks was based in the cloud. But as it hit the headlines few years back, service providers began pulling support [13].

2.3 Data Leakage during Virtual Machine Replication

For providing on-demand service in cloud computing the concept of cloning is used. The process of cloning can cause the data leakage problem associated with machine secrets. Some of the elements of the operating systems such as host keys and cryptographic values are private to a single host. This privacy can be violated by cloning.

2.4 Vulnerability in Virtual-Machine Template Images

Any single vulnerability in virtual-machine template image can spread the vulnerabilities over many systems.

2.5 Owner of Encryption and Decryption Keys

If the data security in cloud is achieved by encryption and decryption mechanisms, the issue arise is who controls the encryption/decryption keys? Is it the customer or cloud service provider? The cloud user usually wants the data to be encrypted when it is at rest in CSP's storage pool. The cloud application design should be such that the corresponding encryption/decryption keys are controlled by the respective cloud user.

2.6 Attacks between Virtual Machines on the Same Server

There may be a case in virtualization in cloud computing which require virtual machines from multiple organizations to be co-located on the same physical resources. Traditional security mechanisms apply to the cloud environment as well, but physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. The access to the administrator is also through the Internet rather than the controlled and restricted direct or

on-premises connection. This increases the risk in cloud security which arise the need to monitor the changes in system control and access control restriction.

2.7 Greater Attack Surface

The cloud applications works on a shared cloud server environment. The virtual machines move between the private cloud and public cloud. That's the main reason that virtual machines are more vulnerable. Thus a cloud environment, which is fully or partially shared, is expected to have a greater attack surface. Therefore it can be considered to be at greater risk than a dedicated resources environment.

3. Information Security

Information security in Cloud Computing depends on three important factors:

3.1 Confidentiality

Confidentiality in cloud ensures that the cloud data of user cannot be accessed by any unauthorized third party.

3.2 Integrity

Encryption of cloud data solves the issue of data confidentiality, but it will not guarantee that the data has not been altered while it resides in the cloud. The integrity factor ensures that the information should not be transformed without evidence of the transformation.

3.3 Availability

Another important factor to be considered is availability of cloud data when it is requested by a authorized cloud user. Here the main concentration is on the threats affecting the availability of data or service.

4. Data Security

Cloud data storage security is an important key factor in the implementation of cloud computing applications [2]. The Cloud Computing still have physical security constraints. When selecting a Cloud provider the cloud user should understand the security protocols of the Cloud Service Provider (CSP). Also the user should understand the things that he/she has to do on his/her end to secure the system against physical vulnerabilities.

4.1 Data Control

In cloud the user's data resides on someone else's servers. The user is unable to see or touch the servers on which their data is hosted [1]. This issue arise the need of controlling the data on remote servers. Additionally the following events could create trouble for cloud user:

- Cloud Service Provider (CSP) fails to secure its infrastructure.
- A third-party sues the cloud provider and takes the control over the cloud infrastructure. The issue becomes more important when there is high probability that the third-party may be a competitor.
- The CSP ceases its operations.

For ensuring the data security and data control we proposed the following solutions. It can be considered that not all solutions could be feasible to implementation of a cloud. For example, the mechanism of encryption could not be suitable for the applications which run over the data in cloud. Because running an application over encrypted data is still a research issue.

a) The CSP must provide the assurance of system and storage protection to the cloud users.

b) The data of cloud users must not be accessed or spoofed by unauthorized users or intruders and also the employees of CSP.

c) The CSP should also provide the assurance of data integrity to the cloud user.

d) When the cloud user plans to adopt the applications of cloud computing, they should evaluate the risk of storage damage, data loss and network security issues on the cloud side.

e) The cloud user should also adopt the physical security specifications to know the physical retrieval procedure of the storage on the cloud.

f) The data in cloud and over communication channels should be kept encrypted to a maximum extent.

4.2 Encryption

The cloud user should encrypt the whole sensitive data in database and in memory also. Decryption of the sensitive data should be done only in the memory only for the time duration for which it is used. Also the user should encrypt the confidential files and data and after that it should be uploaded on the storage provided by the CSP through a secure channel. This mechanism is highly suitable for the data which is not required by the cloud applications and CSP. Also the user should encrypt all the backups and all the network communications [1]. The decryption of user data for the

use of cloud applications is another important point to be considered. Also the issue of executing the cloud applications on the encrypted data, without decrypting it, is also of greater importance. This approach will solve the problem of data security in cloud computing to a much larger extend. The following approaches of encryption can be suggested for providing data security in cloud:

4.2.1 Network Traffic Encryption

To avoid the attacks on the network transmission in cloud computing we can follow the approach to encrypt the entire traffic over the network so that network traffic exchanging data between instances is not visible to other virtual hosts.

One of the approaches of network traffic security is to use Cryptographic IP Encryption (CIPE). CIPE uses the well known cryptographic algorithms Blowfish and IDEA with a key length of 128 bits (like in many other common cryptographic applications, e.g. SSL) [9]. This is commonly believed to be the most secure approach in crypto protocol development. CIPE intercepts the network stack just above the network layer by adding a new network interface. Packets routed through it will be encrypted and put through a tunnel to a peer gateway, where they will be decrypted and delivered [9].

4.2.2 Backup Encryption

Regular backup mechanisms should be provided in order to recover the cloud data even if some unexpected disaster happened at cloud side. The backups should be encrypted using some kind of strong cryptography like PGP. One can then store that backed up data to a cloud storage environment or even in a totally insecure storage.

4.2.3. File System Encryption

Cloud Computing allows an individual to remotely access the data. This remote access provides ease and flexibility to the individuals by freeing them from carrying the data [3]. The data on the cloud may now reside on remote untrusted storage and cross the network boundaries where the network belongs to different administrative domain. This increases the need for securing the remote data.

Remote file access is implemented using Distributed File System (DFS). DFS is a framework for accessing files transparently, where the files are present on different machines over a network. In

this case, when user retrieves a file from the remote server, the file appears as a normal file to the user. User then can work on that file as if the file is accessed locally.

The Cloud Service Provider (CSP) can provide the data security at file system level. This can be done by storing the data in encrypted form by using encrypting file systems. Encrypting file system such as Microsoft EFS [5], eCryptfs [6], Ncryptfs [4], dm-crypt [7], FileVault [8] etc can be used for the same.

All these encrypting file systems work on data security by encrypting and decrypting the data. Also it provides policies such as per-file encryption, sharing of encryption keys etc.

5. Identity and Access Management (IAM)

Identity and Access Management (IAM) can be defined as a method that provide an adequate level of protection for organization resources and data through rules and policies which are enforced on users via various techniques such as enforcing login password, assigning privileges to the users and provisioning user accounts [11].

The basic concepts of IAM are as follows:

a) Authentication:

Authentication is the process of verifying the identity of a user or system.

b) Authorization:

Authorization determines the privileges of the user or a system once the identity is established. Authorization usually follows the authentication step and is used to determine whether the user or service has the necessary privileges to perform certain operations-in other words, authorization is the process of enforcing policies.

c) Auditing:

In the case of auditing, IAM is the process of review and examination of authentication, authorization records, to detect any security breaches in cloud and to suggest the necessary changes that are required in the system in order to avoid the detected security breaches.

6. Conclusion

There are many security issues for cloud computing as it incorporates many technologies like networks, operating systems, databases, virtualization, load balancing, resource scheduling etc. Thus, security issues of many of these technologies also applies to the cloud computing. In this paper, we focused on some major obstacles in cloud computing and also suggested some possible

solutions for the same. We discussed different security issues for cloud computing. These issues include data storage security, network security, application security, network traffic security etc. In order to provide secure cloud environment we discussed different security challenges in cloud computing.

There are many other security challenges like security aspects of virtualization. Due to the complexity of the cloud, it will be difficult to achieve end-to-end cloud security. The main challenge is to have more secure cloud operations even some parts of the cloud fail. Also, maintaining trust between applications from untrusted components will be a major concern involved in cloud computing.

References

[1] George Reese, O'REILLY, "Cloud Application Architectures ".

[2] Chang-Lung Tsai, Uei-Chin Lin, Allen Y. Chang, Chun-Jung Chen, Department of Computer Science, Chinese Culture University, Taipei , Taiwan, "Information Security Issue of Enterprises Adopting the Application of Cloud Computing".

[3] Dharmendra Modi, Rohit Kumar Agrawalla and Rajat Moona, "TransCrypt: A Secure Distributed Encrypting File System", 2010 International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)

[4] C. P. Wright, M. C. Martino, and E. Zadok, "Ncryptfs: A secure and convenient cryptographic file system," in In Proceedings of the Annual USENIX Technical Conference. USENIX Association,2003,pp. 197-210.

[5] "How Encrypting File System Works," Available, http://technet2.microsoft.comlWindowsServer/en/Library/997fdd99-73ec-40419cf41370739a59201033.mspx

[6] M. A. Halcrow,"eCryptfs: An Enterprise-class Encrypted Filesystem for Linux," in Proceedings of the Linux Symposium, Ottawa,Canada, Jul.2005,pp. 201-218.

[7] "dm-crypt: a device-mapper crypto target for Linux," Website, http://www.saout.de/misc/dm-cryptl.

[8] "Apple Mac OS X File Vault", Website, http:// www.apple.com/macosx/features/filevaultl.

[9] http://sites.inka.de/bigred/devel/cipe-faq.html

[10] http://www.hpl.hp.com/techreports /2010/ HPL- 2010 -137.pdf

[11] Sameera Abdulrahman Almulla, Chan Yeob Yeun, Khalifa University of Science, Technology and Research (KUSTAR), Shrjah Campus, Sharjah, United Arab Emirates, "Cloud Computing Security Management"

[12] Trent Jaeger and Joshua Schiffman, The Pennsylvania State University, "Outlook: Cloudy with a Chance of Security Challenges and Improvements", IEEE, January/February 2010.

[13] http://trustandcloudcomputing.org.uk/trust Cloud/default .html

[14] C HENG , D. PaaS-onomics: A CIO's Guide to using Platform-as-a-Service to Lower Costs of Application Initiatives While Improving the Business Value of IT. Tech. rep., LongJump, 2008.

[15] G RAY, J., AND PATTERSON , D. A conversation with Jim Gray. ACM Queue 1, 4 (2003), 8–17.

[16]http://newtech.about.com/od/cloudcomputing/tp/Cloud-Computing-Major-Service-Outages-In-2011.htm