Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8160

Research Paper | Computer Science

Effective Security Controls and Contemporary Issues in Cloud Computing

Mr Dikshan N Shah

Assistant Professor, S S Agrawal Institute of Computer Science, Under the Affiliation of Gujarat Technological University.

ABSTRACT

Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. 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 handling over important data to another company is worrisome. This paper introduces a cloud computing security controls and challenges focusing on the cloud computing types and the service delivery types.

KEYWORDS : Cloud Security Controls, Encryption, Infrastructure.

INTRODUCTION

For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing security or, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There is number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.



Figure 1: Cloud Security

CLOUD SECURITY CONTROLS

Cloud security management addresses issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack.

Deterrent controls

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

Preventative controls

These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

Corrective controls

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

Detective controls

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

CURRENT ISSUES

The main problems cloud computing faces are preserving confidentiality and integrity of data in aiding data security. The primary solution for these problems is encryption of data stored in the cloud. However, encryption of data also brings up new problems. Here is an overview of some of the main problems faced by cloud systems and some solutions.

Trust

Trust between the Service provider and the customer is one of the main issues cloud computing faces today. There is no way for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider.

Legal Issues

There are several regulatory requirements, privacy laws and data security laws that cloud systems need to adhere to. One of the major problems with adhering to the laws is that laws vary from country to country, and users have no control over where their data is physically located.

Confidentiality

Confidentiality is preventing the improper disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems since the information is stored at a remote location that the Service Provider has full access to. Therefore, there has been some method of preserving the confidentiality of data stored in the cloud. The main method used to preserve data confidentiality is data encryption; however encryption brings about its own issues.

Integrity and Completeness

Integrity is preventing the improper modification of information. Preserving Integrity, like confidentiality is another major issue faced by cloud systems that needs to be handled, and is also mainly done by the use of data encryption.

In a common database setup, there would be many users with varying amount of rights. A user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete.

A common approach to such a problem is to use digital signatures; however, the problem with digital signatures is that not all users have access to the data superset, therefore they cannot verify any subset of the data even if they're provided with the digital signature of the superset; and too many possible subsets of data exist to create digital signatures for each.

Encryption
Encryption seems like the perfect solution for ensuring data security; however, it is not without its drawbacks. Encryption takes considerably more computational power, and this is multiplied by several factors in the case of databases. Cryptography greatly affects database performance because each time a query is run, a large amount of data must be decrypted; and since the main operation on a database is running queries, the amount of decryption operations quickly become excessive. There are several approaches developed to handle data encryption; each having its own compromises and downsides, some provide better security mechanisms, and some focus on facilitating more operations to the customers.

Key Management
Since encryption is the main method used to ensure data security, naturally we would be faced with the problem of key management. The encryption keys cannot be stored on the cloud, therefore the customer must manage and control a key management system for any cryptographic method used. For simple encryption schemas such as the "Early Approaches", there might not be a problem since a single encryption and decryption key can be used for the entire system. This simple system to manage keys might even have to take the form of a small database which would have to be a secure local database; which again, may defeat the purpose of moving the original database to the cloud.

Data Splitting
These methods are generally faster than encryption but have their own drawbacks. The idea is to split the data over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original. This method is extremely fast compared to encryption but it requires at least two separate, but homogeneous service providers.

Multi-clouds Database Model (MCDB)
This is a method of Data Splitting which uses multiple clouds and several other techniques to ensure data is split in across clouds in a manner that preserves the data Confidentiality, Integrity and ensures Availability.

MCDB provides cloud with database storage in multi-clouds. MCDB model does not preserve security in a single cloud; rather security and privacy of data will be preserved by applying multi-shares technique on multi-clouds. By doing so, it avoids the negative effects of single cloud, reduces the security risks from malicious insiders in cloud computing environment and reduces the negative impact of encryption techniques

MCDB preserves security and privacy of user's data by replicating data among several clouds, using a triple modular redundancy (TMR) technique with the sequential method. It deals with the cloud manager to manage and control operations between the clients and the multi-clouds inside super cloud service provider.

Multi-Tenancy
Cloud systems share computational resources, storage, services between multiple customer applications (tenants) in order to achieve efficient utilization of resources while decreasing cost, this is referred to as multi-tenancy. However, this sharing of resources violates the confidentiality of tenants' IT Assets. This implies that unless there's a degree of isolation between these tenants, it is very difficult to keep an eye on the data flowing between different realms which make the multi-tenancy model insecure for adoption. Some multi-tenancy issues are:

Virtual Machine Attacks
Typically, in a cloud, business data and applications are stored and ran within virtual machines. These virtual machines are usually running on a server with other virtual machines, some of which can be malicious. Research has shown that attacks against, with and between virtual machines are possible.

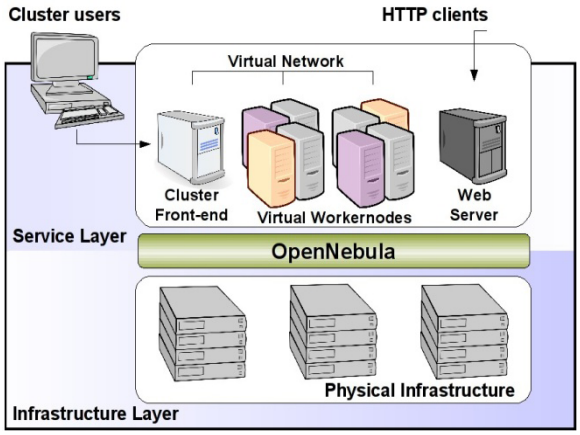

Figure 2: cloud virtual machine

If one of the virtual machines on a server hosts a malicious application that breaches legal or operational barriers; this may lead legal authorities, the service provider or other authorities to shutting down and blocking access the entire server. This would greatly affect the users of the other Virtual Machines on the server.

Shared Resources
Assuming the cloud system isn't running on a virtual machine, the hardware is now an issue. Research has shown that it is possible for information to flow between processor cores, meaning that an application running on one core of a processor can get access to information of another application running on another core. Applications can also pass data between cores.

Multi core processors often have complex and large caches. With these hardware resources, if data is decrypted in the cloud, if even for a moment for comparison, it would then exist unencrypted in the memory of some one of the cloud machines. The problem is that we don't know what other application is running on these machines. Other malicious cloud users can monitoring the machine memory and are able to read our data. However, the likelihood of these hardware attacks is very small.

CONCLUSION
Cloud Computing offers some incredible benefits: unlimited storage, access to lightening quick processing power and the ability to easily share and process information; however, it does have several issues, and most of them are security related. Cloud systems must overcome many obstacles before it becomes widely adopted, but it can be utilized right now with some compromises and in the right conditions.

We have discussed several security issues that currently affect cloud systems. Research is currently being done on the different known issues faced by cloud systems and possible solutions for these issues, however there is still a need for better solutions if cloud systems are to be widely adopted.

One of the main problem that need to be addressed is coming up with a clear and standardized format for the Service Level Agreement (SLA), a format that fully documents all of the services, what services and processes would be provided by the service provider to back up its assurances. When customers have the right level of expectations and the insecurities are deemed manageable, cloud computing as a whole will gain ground and take hold as usable technology.

Another major issue cloud systems face is Encryption. Encryption is the main method of ensuring security of data stored in the cloud; however, encryption is computationally expensive. Encryption methods specific to DaaS (Cloud Databases) has been developed and more research is currently being done on Encryption mechanisms for cloud systems, however, more efficient methods are still needed to help accelerate the adoption of cloud systems.

REFERENCES

[1] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Conference on Hot Topics in Cloud Computing 2009, pages 1-5, USA. | [2] Weis, J., & Alves-Foss, Securing Database as a Service. IEEE Security and Privacy, (2011), Pages 49-55. | [3] Tian Li at el, "Evaluation of User Behavior Trust in Cloud Computing", International Conference on Computer | [4] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security:Routing and DNS security threats | [5] Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia. |