Journal of Information & Communication Technology
Vol. 6, No. 2, (Fall 2012) 48-53

The Analysis of Cloud Computing Major Security Concerns & Their Solutions

Farhat Sharif *
Institute of Business and Technology (IBT)

Abdul Hafeez *
Sindh Madressatul Islam University.

ABSTRACT

Cloud describes the use of a collection of services, applications, information, and infrastructure. It is like a pool of resources and services available in a pay-as-you-go manner. Services like computation, network, and information storage. These components can be organized, specified, implemented, and scaled up or down providing for an on-demand utility model of allocations and compositions (http://en.wikipedia.org/wiki/Cloud-computing, 2012).

With the widespread implementation of cloud computing many organizations have concerns related with their data security. In order to promote the extensive use of cloud, those issues need to be solved. This paper mainly focus on the major security concerns about cloud computing. The major areas of focus are Information Protection, Virtual Desktop Security, Network Security, and Virtual Security.

INSPEC Classification : C5620, C5620W, C5640, C1260C

Keywords : Cloud Computing; Security

1. INTRODUCTION

Cloud computing now becoming the most prominent technology in today's IT world. It is cost-effective, flexible, and scalable in its nature. It can be seen as an integrated technology of today's modern technologies such as grid computing, network storage technology, virtualization, load balancing, and distributed computing. Cloud computing is really successful in reducing cost associated with computing. It was a dream which is now becoming true though it is still in its early stages. In order to gain full advantage of this technology more research work is required. Security is one of the primary issues in this field which need to be overcome and it is becoming a restriction factor in development of cloud computing (Wang Jun-jie, Mu Sen, 2011). My research paper takes a survey and analysis on those security concerns and their possible solutions available in market today.

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (IBT) or Sindh Madressatul Islam University.

* Farhat Sharif : farhatshf@yahoo.com
* Abdul Hafeez : ahkhan@smiu.edu.pk

2. Information Protection

In June 2011, Drop box, a cloud storage provider faced a code change in their authentication system that eliminated user's passwords required to access their data. The result was any one could access any account who he wanted to access. In addition, Drop box was widely criticized for maintaining control of user's encryption keys and compromising those keys fall into wrong hands. Same like, Amazon's Simple Storage Service (S3) faced an HTTP-focused force attack that could expose customer's data storage accounts. These kinds of stories are likely to become common as more applications, systems and data moved into cloud provider environments.

Most IT applications and business operate in the virtual platform. In Cloud computing users can get application services in any place where it has internet, and by any internet terminal. Within virtualized environments, many machines are housed on a single physical system-known as multitenancy. The isolation and segmentation between VMs can be enhanced by virtual Network security appliances or add-ons. However, there are still security challenges that arise from multitenancy, including duties and systems segregation, among others. These include policy, encryption, data loss prevention and monitoring.

a. Policy

In a multitenant environment, such as Cloud, it may not feasible to ensure proper security policy. Different virtual systems and data have different sensitivity levels. Also, data handling and access control may be difficult when migrating systems and applications to a cloud provider. This can be a problem when integrating public cloud services to an existing private cloud (a hybrid cloud scenario), as well as during migration of data and systems to a public cloud environment. For an effective data security policy, this data need to be kept physically separated from others.

b. Encryption

Challenge: Performance issues, key management and maintenance, and access control may make encryption implementation challenging.

Solution: Luckily, various data protection options are rising for cloud environments. In a typical cloud environment data and systems are dynamically migrated across different platforms and distinct data centers. There are a variety of new solution tools available that help organizations to effectively control encryption keys, policies, and authentication and authorization associated with data protection in cloud environment. For example, Amazon Web Services (AWS) has a number of features that allow users to control encryption key and access methods. When new AWS user accounts are created, they are provided an access key. Users can also create X.509 certificates that provide SOAP access to Amazon APIs.

i. File Encryption

Within virtualized and cloud environments the file encryption is the most flexible type of encryptions (Wang Jun-jie, Mu Sen, 2011,). Encryption is applied at the source, and managed by users or third-party providers. Examples of such vendors are Voltage Security and Trend Micro (http://cloudsecurity.trendmicro.com, 2012).

ii. Information Life Cycle in the Cloud

Data lifecycle is another significant area in Cloud information protection. In the case of a business failure or other critical situation, it ensures that customer should have a clearly defined data lifecycle, and also make certain that CSPs can maintain and support encryption. A sound lifecycle approach should include the following:

- Retention (Kresimir Popovic, Zeliko Hocernski, 2010): Cloud Service Providers should state that how long should customer's data retain in a cloud.
- Disposal (Kresimir Popovic, Zeliko Hocernski, 2010): In what circumstances do CSPs dispose of customers data? If something goes wrong on CSPs end then there must be a legal agreement between CSP and customer to protect the customer by stating that CSPs will dispose of data in a secure manner.
- Classification: For sensitive data, organizations must make sure proper segmentation has done by using hypervisor systems.

c. Data Loss Prevention (DLP)

Challenge: Data Loss and Prevention in a Cloud needs a number of various technologies and processes to be effective. Implementing DLP monitoring tools in virtualized environment can be problematic due to resources constraints that result from installation of DLP software agents, or lack of virtualization integration options. Extending DLP to a CSP infrastructure may be difficult, especially in a multitenant environment where granular data protection policies are not available.

Solution: Most major DLP product vendors, including McAfee and Symantec, support DLP agents on Virtual Machines. Trend Micro and Palisade Systems offer DLP virtual appliances that can integrate into virtualized networks.

Challenge: Another challenge faced by cloud-based DLP is the need to tightly integrate into an incident response program. Many CSPs do not provide in house incident response services for customers. This means that any DLP detection or prevention actions taken in the cloud, may not lead to investigations from either CSP or customer IR teams. Unfortunately, major CSPs do not offer robust DLP options that are equivalent to customer's in-house DLP today. The state of data protection capabilities in cloud is still somewhat immature.

Solution: Though new services are growing, but those are currently restricted to email and web traffic. With encryption data can be easily secured with varying numbers of support methods ranging from file and folder encryption to encryption of entire virtual machine.

3. Virtual Desktop Security

Virtual Desktop Security (VDI) improves conformity, information and data protection and malware protection. It offers security teams an automated mechanism for responding to security incidents that is focused on restoring business productivity.

Challenge: The cost of continuous management is increasing, particularly the cost to maintain remote devices. It is also costly to maintain a conforming infrastructure-and as business complexity scales it becomes worse.

Solution: Virtual desktops can always be reached for software maintenance activities such as patches, upgrades and removal of unsupported software's.

VDI not only saves operational expenses, removes obstacles towards increased use of cloud, but it also promotes active desktop security strategies. These strategies include:

a. Reorganize desktop management security

Security executives cannot control when or where malware will smack, but they can control endpoint software configurations to keep the infrastructure conform to security policies and as resistant as possible to infection.

A strategy toward a malware-resistant compliant infrastructure relies upon virtual desktops

to simplify desktop management, reducing the risk of security occurrences and returning operating costs to the business. VDI has the striking properties of creating virtual desktops from centralized images where it is easier for security operations to maintain compliant desktop configurations and to ensure that users operate under the most recent versions of authorized software.

The reduction of operating expenses and increase of productivity is the promise of VDI desktop management strategy. It delivers conform desktop infrastructure to the business.

b. Implement an Automated Data Protection Strategy

The actions taken by virtual desktop in response to security incident include:

- Simplify data leakage prevention, DLP, strategies by restricting sensitive data to the data center with virtual desktops.
- Automatic Backup and recovery of sensitive data through encryption.
- Block of unauthorized flow of sensitive data to unauthorized locations by protecting data by a single copy of a data loss protection (DLP) product.

c. Implant an Active Incident Response Strategy

Being virtualized doesn't mean that attackers won't attack browsers and applications. Security teams can use a proper incident response strategy to mitigate those attacks in order to keep business running.

VDI is gaining attention of most organization to drive the cost out of desktop management and improve flexibility against attacks, thus raising the priority of protecting important information through a coherent incident response plan.

4. Network Security

Cloud computing expanded the network virtualization not only limited to data center but it also provides the ability to user to access the services (distributed geographically) on the cloud using virtualization. This feature changes the cloud computing into dynamic virtual networks.

Challenge: Network conditions such as tenancy, may stop the execution of certain cloud applications in a data centre. Depending on the usage one may need more servers in a certain geographical region.

Solution: To better control user experience a cloud should be distributed across goegraphic regions. An example of this application is Virtual desktop service.

Challenge: The **availability** of information is the most important threat in computing environment (Ramgovind S, Eloff MM, Smith E, 2010). Denial of service attacks is an example of this issue. One would easily attack as more exchange of information takes place. Users must rely on their service providers that they will retrieve what they have stored. This is known as **integrity** issues (Ramgovind S, Eloff MM, Smith E, 2010). Finally, **aggregation** could be the cause of information leakage to third parties. This is case of **confidentiality** issue which is the most important issue as user gets one service place for his business users. So accidental disclosure of information is likely to occur (Ramgovind S, Eloff MM, Smith E, 2010).

Solution: This issue clearly includes a regulatory agreement (Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit, 2009) between the provider and the client so

that clients can trust the provider on the availability and security of data.

Challenge: The attacker can also misuse cloud infrastructre's ability to allocate resources on demand. DoS attacks and spamming are example of these kind of attacks (Farzad Sabahi, 2011).

Solution: These kind of attacks can be identified through Auditing (Ziyuan Wang, 2011) (Kresimir Popovic, Zeliko Hocernski, 2010) .The differentiation between genuine use and misuse is one challenge for automated detection. Auditing might become useful in finding irregularities and detect misuse of infrastructure. Thus can prevent an attack by haling the involved resources.

5. Virtual Security

There are certain important security concerns we need to focus in considering the use of virtualization.

Challenge: One risk is the use of hypervisor. It can be a main target for the attacker if it is weak enough to utilize. Such a risk could have a broad impact if not otherwise alleviated.

Solution: A network isolation and security monitoring exposure is required to overcome this situation.

Challenge: The usage of storage and memory, and allocation and de-allocation of resources over a public cloud are another security concern related with VMs.

Solution: A proper handling and clearance of data should be maintained. Careful handling of operations against sensitive data, and attention to access and privilege controls is required. Verification of released resources would be an excellent security practice.

Challenge: For the VMs located at a physical server it is potential for some undetected attacks between those VMs.

Solution: A verification of no traffic is possible between those VMs can be best approach to mitigate this situation.

The use of virtual local area networks (VLANs) can be a best management practice to isolate traffic flows between VMs. This technique requires wide support for VLANs to be completely effective.

Finally, at cloud flexibility and scale level, this technique must be automated if you have to use virtualization. It must be properly managed and planned in order to take full advantage of this technology.

6. Conclusion

I now close my discussion with the following finding: The cloud computing would become a major commodity just like PC and Internet have brought about information revolution. Nothing, not even security concerns will prevent cloud computing make information affordable and useful. In short it will be 'Unstoppable'.

7. References

Wang Jun-jie, Mu Sen, 2011, "Security Issues and Countermeasures in Cloud Computing".
Ziyuan Wang, 2011, "Security and privacy issues within the Cloud Computing".
Farzad Sabahi, 2011, "Cloud Computing Security Threats and Responses".

Ramgovind S, Eloff MM, Smith E, 2010 "The Management of Security in in Cloud Computing".
http://en.wikipedia.org/wiki/Cloud-computing, 2011
http://cloudsecurity.trendmicro.com, 2011
Kresimir Popovic, Zeliko Hocernski, 2010, "Cloud computing security issues and challenges",
Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit, 2009 "Cloud Security Issues", 2009 IEEE Internal Conference on Service computing.