Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540

Cloud Computing: A Study of Vulnerabilities

Shikha Kuchhal[1]* Ajay Kumar Garg[2]

[1] Assistant Professor, Department of Electronics & Communication Engineering, SPTM

[2] Assistant Professor, University of Delhi

Abstract – Cloud computing is the delivery of different computing services over the internet ('the cloud') such as - software, analytics, servers, storage, databases, networking, and intelligence to offer faster innovation, flexible resources, and economies of scale. The amount is typically paid only for cloud services we use, helping lower our operating costs, run infrastructure more efficiently and scale as our business needs change. Affordable, efficient, and scalable, cloud computing is still the best solution for most businesses -- but it can still leave us vulnerable if the proper precautions aren't taken.

Managers have traditionally viewed IT as difficult and expensive and the promise of cloud computing leads many to think that IT will now be easy and cheap. The reality is that cloud computing has simplified some technical aspects of building computer systems, but the myriad challenges facing IT environment still remain. Organizations which consider adopting cloud based services must also understand the many major problems of information policy, including issues of privacy, security, reliability, access, and regulation. 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 services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications. Pretty much any service that doesn't require you to be physically close to the computer hardware that you are using can now be delivered via the cloud.

Key Words: Cloud Computing, Security Risks, IT Security, Cloud Models, Affordable Computing, Services, Cloud Standards, Risk Assessment

----------X----------

1. INTRODUCTION

Rather than owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider. One benefit of using cloud computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use, when they use it. According to specialists cloud computing is one of the most significant transformation in information technology with many advantages to both companies and end users. Cloud computing is the delivery of different computing services over the internet ('the cloud') such as - software, analytics, servers, storage, databases, networking, and intelligence to offer faster innovation, flexible resources, and economies of scale. The amount is typically paid only for cloud services we use, helping lower our operating costs, run infrastructure more efficiently and scale as our business needs change. Affordable, efficient, and scalable, cloud computing is still the best solution for most businesses -- but it can still leave us vulnerable if the proper precautions aren't taken. 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.

Cloud computing services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications. Pretty much any service that doesn't require us to be physically close to the computer hardware that you are using can now be delivered via the cloud. 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. 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.

Affordable, efficient, and scalable, cloud computing is still the best solution for most businesses -- but it can still leave you vulnerable if the proper precautions aren't taken. Here are six of the most common cloud computing security risks:

a) Distributed-Denial-of-Service Attacks

When cloud computing first became popular, Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable; the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices, smartphones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

b) Shared Cloud Computing Services

Not all cloud hosting solutions and cloud computing services are made equal. Many cloud solutions do not provide the necessary security between clients, leading to shared resources, applications, and systems. In this situation, threats can originate from other clients with the cloud computing service, and threats targeting one client could also have an impact on other clients.

c) Employee Negligence

Employee negligence and employee mistakes remain one of the biggest security issues for all systems, but the threat is particularly dangerous with cloud solutions. Modern employees may log into cloud solutions from their mobile phones, home tablets, and home desktop PCs, potentially leaving the system vulnerable to many outside threats.

d) Data Loss and Inadequate Data Backups

Inadequate data backups and improper data syncing is what has made many businesses vulnerable to ransom ware, a specific type of cloud security threat. Ransomware "locks" away a company's data in encrypted files, only allowing them to access the data once a ransom has been paid. With appropriate data backup solutions, companies need no longer fall prey to these threats.

e) Phishing and Social Engineering Attacks

Due to the openness of a cloud computing system, phishing and social engineering attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can potentially break into a system with ease -- as the system itself is available from anywhere. Employees must be knowledgeable about phishing and social engineering enough to avoid these types of attacks.

f) System Vulnerabilities

Cloud computing systems can still contain system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms. Once vulnerability becomes known with a popular third-party system, this vulnerability can be easily used against organizations. Proper patching and upgrade protocols -- in addition to network monitoring solutions -- are critical for fighting this threat.

Cloud computing security issues are not insurmountable; in fact, many of the risks above can be protected against through the use of a dedicated data protection service. Cloud data protection solutions will both protect data from loss and against cyber security threats, allowing businesses to leverage the power of the cloud without the associated risk.

2. CLOUD DELIVERY MODEL

The technology of cloud computing is based on a modern approach to software engineering called service oriented architecture (SOA). The technique focuses on the delivery of an integrated and orchestrated suite of functions to an end-user trough the use of different functions or services. These services are well defined functionalities that are built as software components and that can be used in different combinations to achieve different goals.

Cloud computing providers offer services built around three fundamental models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), as displayed in the **Figure 1.**

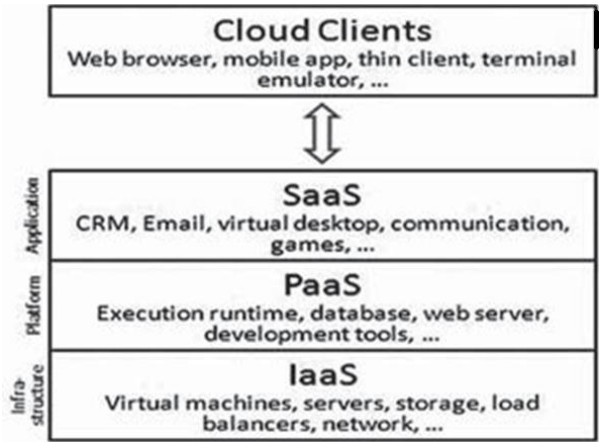

Figure 1: Cloud computing fundamental models

Source: www.wikipedia.com

Infrastructure as a Service (IaaS) is the capability provided to the cloud user that provisions the

processing, storage, networks, and other fundamental computing resources. All of the above enable the user to deploy and run arbitrary applications and even operating system software. The cloud user does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, etc. In this model, it is the cloud user who is responsible for patching and maintaining the operating systems and application software. Infrastructure-as-a-Service is a platform through which businesses can avail equipment in the form of hardware, servers, storage space etc. at pay-per-use service. Examples include Amazon EC2, Terremark Enterprise Cloud, Rackspace, Microsoft Azure, etc.

Platform as a Service (PaaS) is the capability provided to the cloud user to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g. Java, Python, .Net). In such a case the cloud user can develop and run its own software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

Software as a Service (SaaS) represents the capability provided to the cloud user to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin-client interface such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, but only some limited user-specific application configuration settings. Examples include online word processing and spreadsheet tools, customer relationship management (CRM) services and web content delivery services (Salesforce CRM, Google Docs, Yahoo Email, Gmail, etc).

Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. It also raises the question of how it can be properly secured. It is imperative everyone understands their respective role and the security issues inherent in cloud computing.

Cloud service providers treat cloud security risks as a shared responsibility. In this model, the cloud service provider covers security of the cloud itself, and the customer covers security of what they put in it. In every cloud service—from software-as-a-service (SaaS) like Microsoft Office 365 to infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS)—the cloud computing customer is always responsible for protecting their data from security threats and controlling access to it.

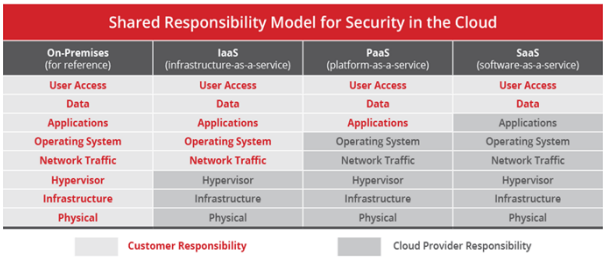

Figure 2: Shared responsibility for security between cloud providers and their customers.

Most cloud computing security risks are related to cloud data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues come back to the data customers put in the cloud. Read below for an analysis of the top cloud security challenges in SaaS, IaaS, and private cloud, placed in order by how often they are experienced by enterprise organizations around the world.[1]

3. CLOUD DEPLOYMENT MODELS

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways :

a. **Private Cloud** — the cloud infrastructure has been deployed, and is maintained and operated only for a specific organization. The cloud may be hosted within the organization or externally and is managed internally or by a third-party. This model does not benefit from the less hands-on management, nor from the economic advantages that make cloud computing such an intriguing concept.

b. **Public Cloud** — the cloud infrastructure is made available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial implications compared to the capital expenditure requirements normally associated with other deployment options.

c. **Community Cloud** — the cloud infrastructure is shared among a number of organizations with similar interests and requirements. It can be managed internally or by a third party and hosted within the organization or externally. The costs are shared among fewer users than a public cloud. Hence a community cloud benefits from medium costs as a result of a sharing policy. By means of comparison, with the

private cloud the costs increase alongside the level of expertise needed.

d. Hybrid cloud is a combination of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without being entirely dependent on third party services. Hybrid Cloud architecture requires both on-premises resources and off-site (remote) server based cloud infrastructure. Hybrid clouds lack the flexibility, security and certainty of in-house applications. However, they provide the flexibility of in-house applications with the fault tolerance and scalability of cloud based services.

4. VULNERABILITIES OF ADOPTING CLOUD COMPUTING TECHNOLOGY

The process of creating and managing a secure cloud space is a more challenging task than creating a secure classical IT environment. Given the immaturity of this technology the new resources and the reallocation of traditional ones are not fully tested and come with new risks that are still under research.

The main risks of adopting cloud computing identified by this paper are:

a. Misunderstanding responsibilities.

If in a traditional scenario the security of data is entirely the burden of the company owning data. In the cloud computing scenario the responsibilities are divided between the two actors: the cloud provider and the client. There is a tremendous potential for misguided risk management decisions if cloud providers do not disclose the extent to which the security controls are implemented and the consumer knows which controls are further needed to be adopted.

Different kinds of cloud services adopted mean different responsibilities for the service provider and the customer. If an IaaS service model is adopted, then the provider is responsible for physical security, environment security and the virtualization software security, whereas the consumer is responsible for securing everything else above this layer including operating system, applications and data. However, in an SaaS cloud service model the provider is responsible not only for the physical and environmental security but also for all the software services he uses in order to provide that particular software service to the client. In this case, the responsibilities of the consumer in the field of security are much lowered.

b. Interoperability issues

The cloud computing technology offers a degree of resource scalability which has never been reached before. Companies can benefit from additional computational needs, storage space, bandwidth allocation, etc. whenever they need and without great investments to support peak load demands. If the demand falls back the additional capacity can be shut down just as quickly as it was scaled up without any hardware equipment sitting idle.

This great advantage has also a major drawback. It comes alongside with the risk of managing data within a shared environment (computation, storage, and network) with other cloud clients. Additionally, at one time one company may have multiple cloud providers for different services which have to be interoperable. In time, for different reasons, companies may decide to move their services to another cloud and in such a case the lack of interoperability can block or raise heavy obstacles to such a process.

c. Data security and confidentiality issues

One of the biggest security concerns people have when moving to the cloud is related to the problem of keeping data secure and confidential. In this respect, some particular problems arise: who can create data, where the data is stored, who can access and modify data, what happens when data is deleted, how the back-up is done, how the data transfer occurs, etc. All of this is known as data security lifecycle and it is displayed in **Figure 2**.

Figure 3: The data security lifecycle Source: www.securosis.com

This lifecycle exists also in the classic architecture but in a cloud environment its stages are much more complex, posing higher security risks and requiring a more careful management. Worth reminding in this respect is that it is much more difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus be sure that the data is handled in a proper way.

To counter such a risk, strategies like data encryption, particular public key infrastructure, data

dispersion, standardization of APIs, etc are proposed to customers as security measures to create a trusted and secure environment.

d. Lack of Standards

The immaturity of this technology makes it difficult to develop a comprehensive and commonly accepted set of standards. As a result, many standard development organizations were established in order to research and develop the specifications. Organizations like *Cloud Security Alliance, European Network and Information Security Agency, Cloud Standards Customer Council,* etc. have developed best practices regulations and recommendations. Other establishments, like Distributed Management Task Force, The European Telecommunications Standards Institute, Open Grid Forum, Open Cloud Consortium, National Institute of Standards and Technology, Storage Networking Industry Association etc., centered their activity on the development of working standards for different aspects of the cloud technology. The excitement around cloud has created a flurry of standards and open source activity leading to market confusion. That is why certain working groups like Cloud Standards Coordination, TM Forum, etc. act to improve collaboration, coordination, information and resource sharing between the organizations acting in this research field.

e. Reliability breakdowns

Another important aspect of the cloud computing is the reliability or availability of services. The breakdown of an essential service operating in a cloud has an impact on many clients. For example, in April 2012 there was a Gmail disruption that made Gmail services unavailable for almost 1 hour. The company first said that it affected less than 2 % of their customers, then they updated to 10 %, which sums around 35 million clients of a total of 350 million users. These incidents are not rare and evidence the customer lack of control over their data.

Also, in this industry, the leading companies have set some high level quality services. Those levels are not easy to be reached by the other cloud service providers which do not have such a well-developed infrastructure. Unfortunately for the clients these quality services may come at higher costs and sometimes the decision makers, lured by the cheaper services, will be reluctant to collaborate with such a provider.

Cloud environments experience--at a high level--the same threats as traditional data center environments; the threat picture is the same. That is, cloud computing runs software, software has vulnerabilities, and adversaries try to exploit those vulnerabilities. However, unlike information technology systems in a traditional data center, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the CSP and the cloud consumer. As a result, consumers must understand the division of responsibilities and trust that the CSP meets their responsibilities. Based on our literature searches and analysis efforts, the following list of cloud-unique and shared cloud/on-premise vulnerabilities and threats were identified. The figure below also details the threat picture for cloud computing platforms.

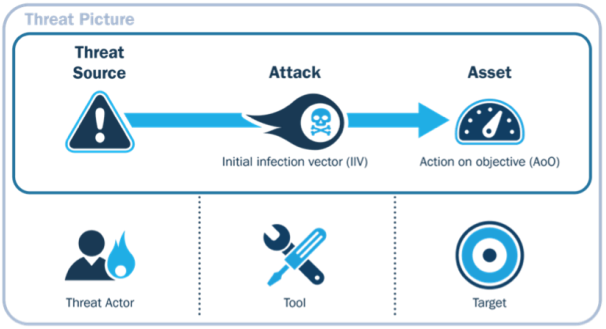

Figure 4: Cloud-Unique Threats and Risks

5. CONCLUSIONS

Securing the cloud is a shared responsibility between the cloud service provider (CSP) and the enterprise. The amount of responsibility per entity is dependent upon which cloud service the enterprise uses and whether it is a public, private, or hybrid cloud. Service-level agreements should detail what an enterprise is and is not responsible for when it comes to security. “Cloud” computing is based on technologies like virtualization, distributed computing, grid computing, utility computing, but also on networking, web and software services. The benefits of adopting this technology draw decision makers’ attention and nowadays many companies are engaged in adopting or researching cloud adoption. Specialists who analyze this sector forecast that the global market for cloud computing will experience a significant increase in the next years and will replace traditional IT environment.

In the process of adopting cloud based services companies and IT organizations should evaluate the business benefits and risks. The cloud’s economies of scale and flexibility are both a friend and a foe from a security point of view. The management of security risk involves users, the technology itself, the cloud service providers, and the legal aspects of the data and services being used. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective than traditional ones. To help reduce the threat, cloud computing stakeholders should invest in implementing security measures to ensure that the data is being kept secure and private throughout its lifecycle.

REFERENCES

1) Bob Savage's speech delivered to Science Foundation Ireland's (SFI) forum, 'Science and Industry: Working Together for Economic Recovery',

2) Cloud Computing Security Issues, Florin Ogigau-Neamtiu, The Regional Department of Defense Resources Management Studies, Brasov, Romania

3) http://www.siliconrepublic. com/cloud/item/24428-cloud- most-significant-tran, last retrieved 02.08.2012

4) http://wikipedia.org/wiki/Cloud_ computing last retrieved 04.08.2012

5) http://www.vmware.com/ solutions/cloud-computing/index.html, last retrieved 02.08.2012

6) https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

7) https://securosis.com/blog/data- security-lifecycle-2.0 last retrieved 15.08.2012

8) http://www.redhat.com/solutions/ cloud-computing/, last retrieved 15.08.2012

9) https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

10) http://softwarestrategiesblog. com/2012/01/17/roundup-of-cloud-computing-forecasts-and-market- estimates-2012/, last retrieved 29.07.2012

11) http://www.google.com/appsstatus, last retrieved 16.08.2012

12) http://cloud-standards.org, last retrieved 10.08.2012

13) http://cloud-standards.org/wiki/ index.php?title=Cloud_standards_ overview, last retrieved 13.08.2012

14) http://royal.pingdom.com/2007/09/26/google-availability-differs-greatly-between-countries/, last retrieved 27.08.2012

15) http://www.techrepublic. com/blog/datacenter/11-cloud-iaas- providers-compared/5285, last retrieved 05.08.2012

Corresponding Author

Shikha Kuchhal*

Assistant Professor, Department of Electronics & Communication Engineering, SPTM