CLOUD COMPUTING CHALLENGES: SECURITY MEASURES IN REAL TIME WEB APPLICATION

Indravadan S. Patel*

Sonal J. Patel*

ABSTRACT

Cloud Commuting are multi tier application that provide the facility to end user without installing any software, server and database for using any web based application except live internet connection and any compatible browser. Cloud computing provides web based solution to end user, business user or any organization globally solution and access from anywhere as per their rights. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computer. In some cases, legacy applications are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data centre location. In other cases, entire business applications have been coded using web-based technologies such as AJAX For the advancement of the end user facility all the business logic and data are stored at one place either it is form of private, public or hybrid cloud. So there are some security aspect of challenges like virus attacking from end user, Data Protection, Identify Management, physical security and etc.

Keywords: *Cloud Technologies, AJAX, Cloud Computing Security.*

*Assistant Professor, Department of Computer Science, Ganpat University, Mehsana, Gujarat, India.

1. INTRODUCTION

Everyone has an opinion on what is cloud computing. It can be the ability to rent a server or a thousand servers and run a geophysical modeling application on the most powerful systems available anywhere. It can be the ability to rent a virtual server, load software on it, turn it on and off at will, or clone it ten times to meet a sudden workload demand. It can be storing and securing immense amounts of data that is accessible only by authorized applications and users. It can be supported by a cloud provider that sets up a platform that includes the OS, Apache, a MySQL database, Perl, Python, and PHP with the ability to scale automatically in response to changing workloads. Cloud computing can be the ability to use applications on the Internet that store and protect data while providing a service - anything

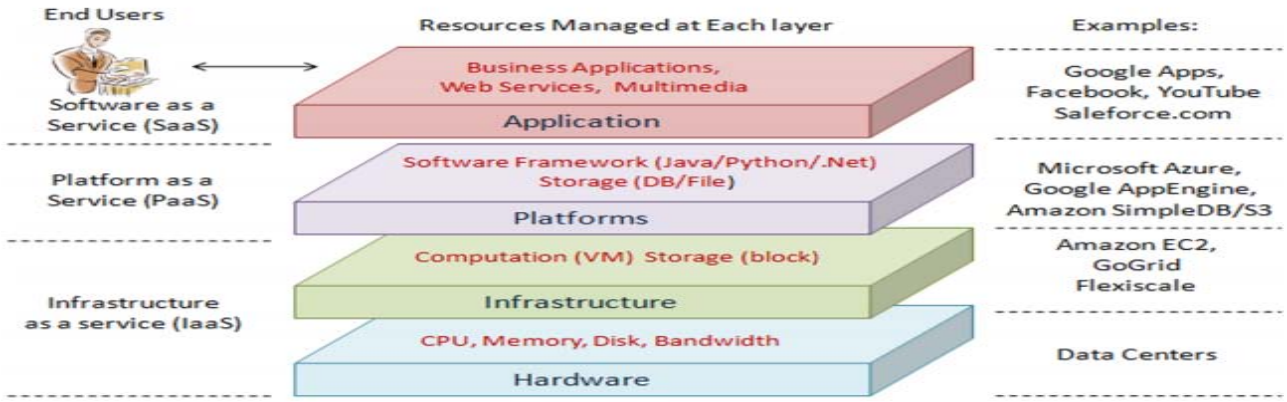
Including email, sales force automation and tax preparation. It can be using a storage cloud to hold application, business, and personal data. And it can be the ability to use a handful of Web services to integrate photos, maps, and GPS information to create a mash up in customer Web browsers. [1].

In a cloud computing environment, the traditional role of service provider is divided into two: the infrastructure providers who manage cloud platforms and lease resources according to a usage-based pricing model, and service providers, who rent resources from one or many infrastructure providers to serve the end users. The emergence of cloud computing has made a tremendous impaction the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm. Indeed, cloud computing provides several compelling features that make it attractive to business owners, as shown below [2].

- Zero investment
- Lowering operating cost
- Highly scalable
- Easy access
- Reducing business risks & maintenance expenses

2. CLOUD COMPUTING SERVICE MODEL

FIG 1. CLOUD COMPUTING ARCHITECTURE



Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but does control the deployed applications and possibly application hosting environment configurations.

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [3].

3. DEPLOYMENT MODEL

Private: Private Clouds are provided by an organization or their designated service provider and offer a single-tenant (dedicated) operating environment with all the benefits and

functionality of elasticity and the accountability/utility model of Cloud. The physical infrastructure may be owned by and/or physically located in the organization's datacenters (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively. The consumers of the service are considered "trusted." Trusted consumers of service are those who are considered part of an organization's legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Public: Public Clouds are provided by a designated service provider and may offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of Cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's datacenters (off-premise.) Consumers of Public Cloud services are considered to be untrusted.

Managed: Managed Clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability /utility model of Cloud. The physical infrastructure is owned by and/or physically located in the organization's datacenters with an extension of management and security control planes controlled by the designated service provider. Consumers of Managed Clouds may be trusted or untrusted.

Hybrid: Hybrid Clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate Cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. This model provides for an extension of management and security control planes. Consumers of Hybrid Clouds may be trusted or untrusted [4].

4. CLOUD SECURITY MEASURES

Cloud security considered on different levels. Services provider and data storage adhere on security challenges.

- Cloud Provisioning Services.
- Cloud Data Services.
- Cloud Processing Infrastructure.

- Cloud Support Services.
- Cloud Network and Perimeter Security [5].

Data Protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

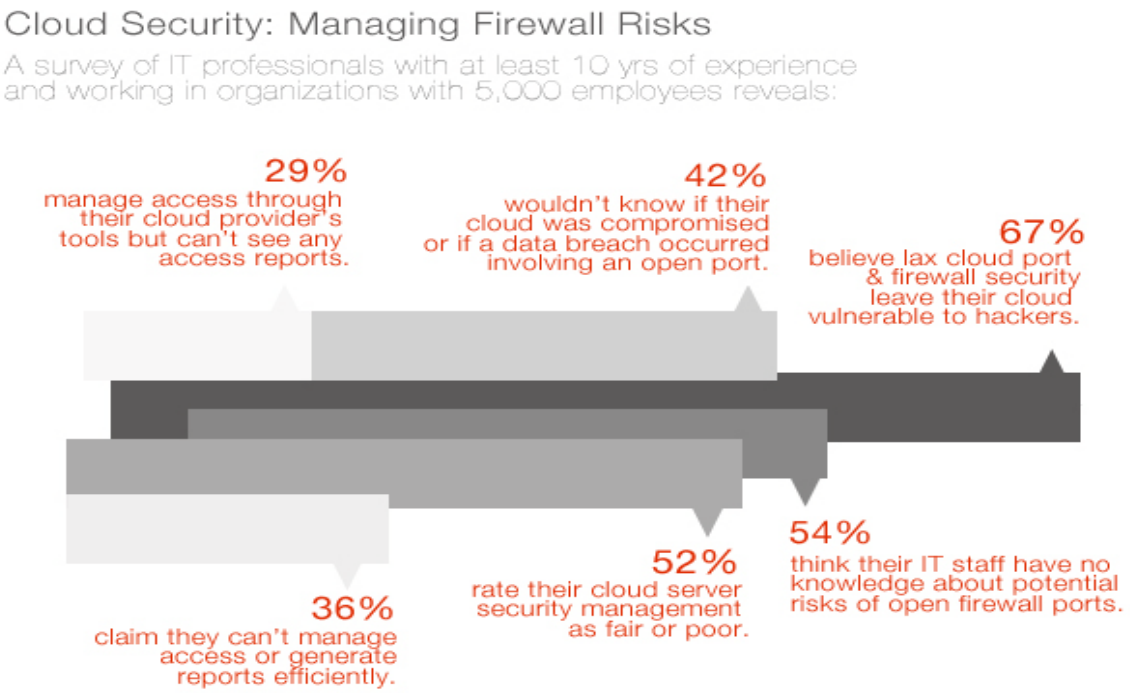
Insecure or Incomplete Data Deletion: when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

Malicious Insider: while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers [6].

Attacks on Cloud Services: In cloud services various attacks are mounted by different users like Danial of Service, QoS Violation, Man in Middle Attack, IP Spoofing, Port Scanning, ARP Cache Attack [7].

5. FIREWALL RISKS

Fig 2: Cloud Security Survey on Firewall Risks



A recent cloud computing security study conducted by the Poneman Institute and sponsored by Dome9 reveals that 67 percent of IT professionals claim their organization is left vulnerable to hackers due to lax cloud port and firewall security. Fifty-two percent of respondents rated their organization's overall cloud server security management as fair (27 percent) or poor (25 percent).

In addition, 54 percent of respondents to the study said their IT staff had no knowledge about the potential risks of open firewall ports in their cloud environments. These significant statistics show a major lack of security concerns among IT personnel that ultimately affect clients' data and applications in the cloud.

Even more alarming are the 42 percent of the respondents that fear they wouldn't know if their data or applications on their cloud were actually compromised or if a data breach occurred, involving an open port on a cloud server [8].

6. CONCLUSION

While Security emerges as a major concern among those who respond to cloud computing surveys, the key to understanding security in cloud computing is to realize that the technology is not new, or untested. It represent the logical progression to outsourcing of commodity services to many of the same trusted it providers we have already been using for

years. Examples of previous cloud computing capabilities include hosted mainframe hosted file and mail servers and software services.

This paper address some of the security issues in cloud computing. Cloud security is part of the inevitable progression of it. It must be embraced by organization to stay coemptive. Companies who approach clod computing in a mature manner need not be afraid about entering the cloud environment because of security concern. Dealing with security in the cloud is no more difficult that addressing it internally.

7. REFERENCES

[1] Introduction to Cloud Computing Architecture, Sun Micro System, Technical Report 2009.

[2] Cloud computing: state-of-the-art and research Challenges, Qi Zhang · Lu Cheng · Raouf Boutaba

[3] Cloud Computing Security, A Trend Micro White Paper, May 2010

[4] Cloud Computing [Security] Architectural Framework http://www.rationalsurvivability.com /blog/?cat=284

[5] Top five cloud computing security issues http://www.esecurityplanet.com /trends/article.ph p/3930401/Top-5-Cloud-Computing- SecurityConcerns.htm.

[6] Cloud Computing, Benefits, risks and Recommendations for information security, ENISA, Nov 2009

[7] Towards Cloud Computing- Security Issues and Challenges, IJ-CA-ETS Sept 2011

[8] Study on Cloud Computing Security: Managing Firewall Risks. http://resource.onlinetech.com/study-on-cloud- computing-security-managing-firewall-risks/.