CLOUD COMPUTING: CHALLENGES OF SECURITY ISSUES

Mousmi Ajay Chaurasia
Information Technology Department, M.J.C.E.T. Hyderabad

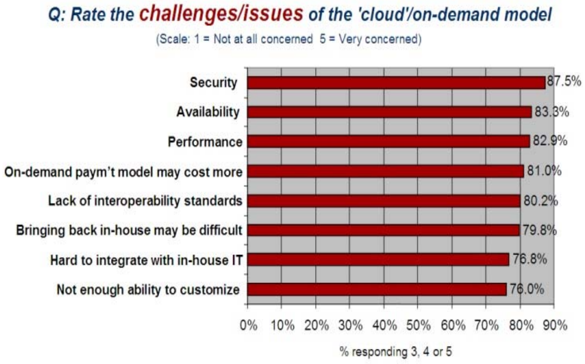
ABSTRACT

Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through Internet, based on pay-as-you-go approach. It is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Cloud computing provides number of benefits out of which economic benefit is main benefit. With the lots of benefits some challenges are there to be solved and out of which security is a major challenge. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud security issue is a critical issue and because of this users are hesitating to use the clouds. In this paper we surveyed a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types. Our main contribution is to classify the issues according to the different service models and to provide some directions for solutions. Enough or adequate security can be achieved by solving these issues.

Keywords: Cloud computing security, IT, Scalability

1. 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 encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure 1.



Source: IDC Enterprise Panel, 3Q09, n = 263

Figure 1: Results of IDC survey ranking security challenges, 2008 [1]

Cloud computing environments are likely to suffer from a number of known vulnerabilities, enabling attackers either to obtain computing services for free (attack against cloud providers), steal information from cloud users (attack against cloud customers data), or penetrate the infrastructure remaining in client premises through cloud connections (attack against cloud customer infrastructures). Typical examples of these attacks today are VoIP free calls, SQL injection, and drive by downloads [2]. Cloud networking will not change the fact that vulnerabilities will continue to exist and that attackers will continue to exploit them [3].

Big IT giants like Google, Amazon, and salesforce.com are providing computing facility like storage, computation and application by pay as per usage through Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud service models. Since cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it's more prone to security threats and vulnerabilities. Security issues are of more concern to cloud service providers who are actually hosting the services.

The rest of the paper is organized as follows: in section 2, Cloud Computing Architecture has been described. We have discussed few security challenges with its solutions in section3. In section 4 we have concluded the paper.

2. CLOUD COMPUTING ARCHITECTURE

Cloud Service Models [4, 5] simply mean what type of services can be provided to customers. Cloud * as a Service, where * can be replaced by any one of the following: Desktop, Security, Data, Software, Platform, Infrastructure, IT, Testing, Hardware, Computing, Database, Storage etc.

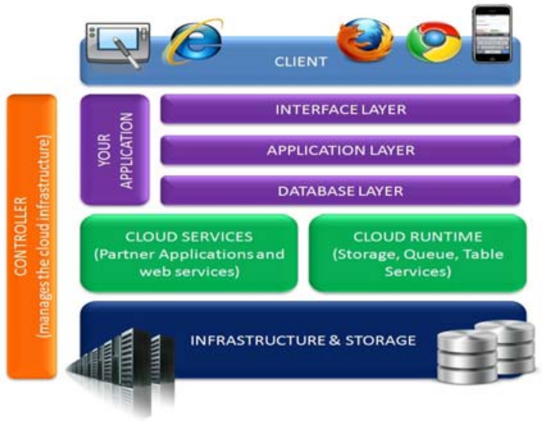

CLIENT
INTERFACE LAYER
APPLICATION LAYER
DATABASE LAYER
YOUR APPLICATION
CLOUD SERVICES (Partner Applications and web services)
CLOUD RUNTIME (Storage, Queue, Table Services)
INFRASTRUCTURE & STORAGE
CONTROLLER (manages the cloud infrastructure)

Figure 2: Cloud Computing Architecture

Cloud Computing can be broadly classified into three categories, i.e., three layers of Cloud Stack, also known as Cloud Service Models or SPI Service Model:

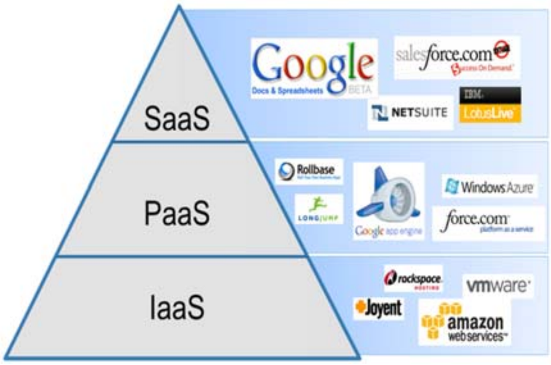


Figure 3: Cloud Service Models

2.1 SAAS

SAAS is a software model provided by the vendor through an online service. It provides network-based access to commercially available software. User interface powered by "thin client" applications; cloud components; communication via (Application Program Interfaces (APIs); stateless; loosely coupled; modular; semantic interoperability. This will avoid capital expenditure on software and development resources; reduced Return On Investment (ROI) risk; streamlined and iterative updates. On the contrary, Centralization of data requires new/different security measures. Examples of SaaS include Netflix, Intuit QuickBooks Online, Gmail, and Google Docs. The four major advantages of Saas are:-

- Increased speed of deployment
- Increased user adoption
- Reduced support requirements
- Lowered cost of implementation and upgrades

2.2 PAAS

PaaS enables companies to develop applications more quickly and efficiently in a cloud environment using programming languages and tools supported by the provider. The defining factor that makes PaaS unique is that it lets developers build and deploy web applications on a hosted infrastructure. It consumes cloud infrastructure. Every centralized system requires new/different security measures. Common examples of platforms include Windows™, Apple Mac OS X, and Linux for operating systems; Google Android, Windows Mobile, and Apple iOS for mobile computing; and Adobe

AIR or the Microsoft .NET Framework for software frameworks.

2.3 IAAS

This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. Usually platform-independent; infrastructure costs are shared and thus reduced; service level agreements (SLAs); pay by usage; self-scaling. Avoid capital expenditure on hardware and human resources; reduced ROI risk; low barriers to entry; streamlined and automated scaling but disadvantages are Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater long-term cost; centralization requires new/different security measures. With , a company can rent fundamental computing resources for deploying and running applications or storing data. IaaS enables fast deployment of applications, and improves the agility of IT services by instantly adding computing processing power and storage capacity when needed.

2.4 CLOUD DEPLOYMENT MODELS

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services:

- *Public Cloud:* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Means where the infrastructure resides totally outside of the tenant / enterprises?
- *Private Cloud:* The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises. IT services are mounted on top of large-scale accumulated and virtualized infrastructure within enterprise firewall and consumed in “per transaction” basis.
- *Community Cloud:* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance. considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.
- *Hybrid Cloud:* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Here, the infrastructure and business processes reside partly within the enterprise and partly consumed from third party.

The most challenging threat in cloud computing is security issues. Security can be compromised in terms of hacking the available data, by disturbing some issues to slow down the server (i.e. Performance) etc. We recognize that there are three major groups involved in cloud security:

First group is the providers of Public and Hybrid clouds. *Second group* is the individuals / organizations which use cloud services - either by migrating and hosting their applications binaries / data to cloud, or by having an interface or a “pipe” connected to an external cloud to do some activities (like downloading cloud public data/ modules or to route messages through cloud).

The Third group is the Government and other third-party regulatory entities that may have fiduciary roles (audit, forensic etc.).

While some cloud security works [6] focus on legal and jurisdictional risks, some institutions provide valuable recommendations for increasing cloud security [7, 8] from a more technical point of view.

3. CLOUD COMPUTING SECURITY ISSUES

Cloud computing is steadily gaining acceptance within businesses. It is predicted that by 2018, 59% of the cloud workloads will be generated from Software as a Service (Saas). Cloud Computing has already started to revolutionise the way we store and access data. We currently see smartphone applications use cloud computing technology to allow users to store and access data they previously couldn’t on a smart device[18].

In clouds rather than other issues security is the biggest issue. Due to this issue users are hesitating to use the clouds. According to a survey mentioned in [9] which is done in 2011 shows that 36% lack of cloud computing usage is due to security concerns. By Securing the Saas, PaaS and IaaS security issues indirectly we can secure the cloud system. Enough or adequate security can be achieved by solving these issues. Information security, Virtualized environment security issue and Communication security issues are some related issues. Information security is related to the important aspects of Availability, Confidentiality, and integrity. Rather than these issues, Trust, Governance, Legal and Virtual Machine security issues are also should be in focus.

3.1 INFORMATION SECURITY ISSUES (SAAS, PAAS, IAAS*)*:

3.1.1 Availability:

Availability means to ensure that users can use these services at any time at any place. It means availability of the infrastructure, software, or the data. All the Cloud computing systems like SaaS, PaaS, IaaS etc allows their users to access the cloud at anytime any place, to achieve this, cloud services should be available all the time.

Virtual machines have capability to provide on demand services in terms of users. Most of the cloud computing systems provide cloud infrastructures and platforms based on virtual machines e.g. Amazon, S3, Xen so on. Amazon is using the virtual machines to rend resources (e.g. CPU cycles, storage capacity, memory etc.) [10].

The availability of the provided infrastructure can be enhanced by solidifying the security controls strategies such as offering the ability to block and filter traffic based on IP address and port only to secure their systems such strategies are offered by current cloud computing system vendors like Amazon, skytab [10].

Redundancy is another technique to provide the availability of the cloud. It means having multiple copies of the same data. Redundancy enhances the availability of the data or the system. Amazon and Google use this policy to provide availability [10].

3.1.2. CONFIDENTIALITY AND PRIVACY:

It means the data belongs to a particular user and it should not be revealed to any unauthorized party. It means only authorized parties or the systems can access to the data. As cloud systems have web-native nature and it is business oriented in which resources are shared which increases the risk of data compromise. It can be easily correlated to user authentication.

One option for enhancing the confidentiality is encryption of the data. Encrypted data will be more secure rather than unencrypted. A health care company TC3 is successfully using this approach [10]. A Homomorphic cryptography (HC) can meet encryption challenge. Homomorphic Cryptography ensures that operations performed on an encrypted text results in an encrypted version of the processed text. But till date it is having just a theoretical value [13].

Encryption technique works while data is in transit mode. One question arises that what about the security of the data stored on the data storage device at the cloud provider. A good solution for this question has been given by [10] is Tokenization. Tokenization means replacing sensitive data by dummy token. Translation of the token can be done at the client endpoint or at separate cloud provider.

***Privacy*:** Privacy is a desire of a person to disclosure of personal information. In clouds the data is stored on service provider's server which can be anywhere in the world and it has to follow or obey the privacy and confidentiality laws of that country where the server is placed [12]. Privacy can be affected by hacking users' account, erroneous manipulations, data stolen, phishing, deletion of data. Cloud computing is often prone to malicious insiders either by account hacking or through service.

Easily less compromised, stronger, more secure than a static password is a Two-Factor authentication solution. Two factors typically are 'something you know like pin code or password' and 'something you have like hardware token, mobile phone, and finger print etc'. It includes like One-Time password (OTP), a digital certificate and biometric verification [13].

Weak authentications can be the cause of breach in privacy. If the users identification is done electronically and presented to an information system can establish confidence in user identities [12].

As said in [9] the vertica has used Virtual Private Network (VPN) and firewall for its data lose security rather than VPN port and Software they blocked off all external communication.

3.1.3. INTEGRITY

Integrity means modification of data, referring of data, software and hardware. Integrity can be done only by authorized parties and in an authorized ways. Integrity is a key aspect of security in cloud computing systems. It is also related to data loss and data stolen. As cloud systems are based on virtual machines, access points and number of entities is increased and due to this integrity assurance and accuracy becomes crucial. One prominent solution discussed in [11] is using of Zetta systems of storage which implements the Rain-6. Rain-6 is capable of recovering network failure, hard disk failure or corruption, power supply shortage etc it is able to tolerate three simultaneous failures (e.g. three disks failure or even a three entire nodes failure). Adding digital signature to the data enhances the data integrity (e.g. GFS (Google file system) and HDFS use this technique).

Software integrity is also needed in cloud systems and it can be achieved by handing over to the software's owner or administrator. Same the hardware also have to protect from unauthorized access and this issue should be addressed to cloud providers.

A company which is using cloud to host their data can achieve the data integrity by giving rights or privileges to its users or employees. Privileges for modification, deletion and fabrication [12]. If a user is having the privilege to view the data means it can't do any changes in data. By providing such kind of privileges to users, the system can achieve greater confidence in data and system integrity.

Instead of following the solutions of the issues in data confidentiality, integrity, authenticity of data and communications individually one solution can be used for all that is trusted third part. It provides secure interactions between two parties who both trust this third party [12]. The trusted third party from [12] can be relied upon for:

- Low and high level confidentiality.
- Server and client authentication.
- Creation of security domains
- Cryptographic separation of data
- Certificate based authorization

SaaS application's functionality is based on APIs. Ws-Transaction and WS-Reliability standards are available for managing data integrity with web services ,but these services are not yet matured and not many vendors have implemented these [14]. Architects, developers and cloud providers should make sure that they do not compromise data integrity in their eagerness to move the cloud computing [14].

3.2. IAAS

The security issues in Infrastructure as a Service are just can be addressed as physical security, environmental security and virtualization security. IaaS in public cloud poses the major risk whereas private cloud seems to have lesser impact. IaaS is prone to have various degrees of security. Infrastructure is also pertains to the transmission path including the hardware where data is stored. There is a high possibility that data can be routed through an intruder's infrastructure, because in cloud environment data is transmitted through umpteen number of third party infrastructure devices [13]. The security concerns which are threatening the internet also threaten the cloud because cloud computing system uses the same normal underlying internet technology to transmit the data. According to [14] a robust set of policies and protocols are required to help secure transmission of data within the cloud.

Security can be affected through Virtual Machines (VM) and it can be happen during communications between VMs and host, communication between VMs, VMs mobility and Denial of Service (DoS). While sharing resources, applications transfer between VMs a malicious VM can exchange data.

The system administrator or any authorized party who has a privilege to monitor the virtual machines like start, shutdown, pause, restart of the machine etc, resource modification etc can misuse the privilege. A solution for this is Xenaccess, a tool which allows system administrator to run a user level process in Dom0 (a privileged domain in Xen) , Amazon EC2 and Citrix are examples [15]. In clouds virtual machines can transfer the data between virtual machines and hosts, attackers can use this feature to exchange data between cooperating malicious programs in virtual machines. Trusted virtual Datacenters (TVDC) implements management prototypes that demonstrate isolation constraints and integrity check [15].

DoS is critical threat to VMs and it can be happen do to wrong or miss configuration of hypervisor. Due to this threat a single VM can consume all the resources. Automatic restart of the VM can help the hypervisor to take suitable solutions.

3.3. PAAS

In PaaS provider might give same control to the people on the top of platform but host and network intrusion prevention will still be in the scope of the provider and provider should give the assurance that data remains in accessible between applications. Various malicious activities over cloud platform can cause network intrusion [9]. This problem can be solved by using Multi Protocol Label Switching (MPLs), Virtual Private Network (VPNs) and Virtual-Area Networks (VLANs) same of the best strategies. This process ensures that the devices can only access a virtually secured network that is free of possible intrusions [9].

Virtualization environment security issues are related to PaaS and are like isolation of virtual machines; information theft through malicious use of hypervisor, distrusted hypervisor, distrusted virtual machines. [13]. Solutions for these issues are selection of the right hypervisor can solve isolation of virtual machines. Encrypting a virtual machine is a potential solution [13].

Rather than all these issues discussed above we can’t forget to mansion the trust, governance, legal and virtual environment aspects and legal intercepts. They might pass legal borders due to the fact that virtual components can move to arbitrary physical cloud networking infrastructure.

3.3.1. TRUST

Trust means users have reliability over the cloud providers that they will act exactly as expected and required and their data is safe on the cloud. Users are lacking trust over cloud computing systems and even cloud providers are getting failed to make users trust them. Due to increased level of abstraction perceived by cloud consumers, loses visibility. The users are unknown of what is happening with their data, because of multi tenancy there is also limited control over how resources are shared practically it is very difficult to provide traditional client audits or reviews to provide the expected level of assurance.

Use of third parties will be helpful for gaining trust of the users on cloud computing systems [12].

3.3.2 GOVERNANCE

Governance means keeping control and oversight over policies, procedures and standards for application development. Basic issues of governance in cloud computing is related to identification and implementation of appropriate organizational structures ,process and controls to maintain effective information security governance, risk management compliance [16].

This problem can be solved by including security metrics and standards in Service Level Agreements (SLA) and contracts. While a SLA is going to establish, security department should be engaged to ensure that security requirements are contractually enforced [16].

3.3.3 LEGAL ISSUES

Geographical locations are not fixed for any resources in the clouds. They may migrate between the physical locations due to the different factors and reasons. Because of the migration they may come under multiple legal jurisdictions and these jurisdictions may have conflicting rules about security issues such as intrusion and data protection [17].

Make sure that the migration rules, country location restrictions are defined and enforced or mentioned in SLA or contract. SLA is the only legal agreement between the service provider and the client. Providers should assure customer that their data is safe, authentic. They should have mutual understandings between them. Rules should be mentioned in SLA regarding expected or unexpected transmission of contract. Legal intercepts are not classical attacks but they might violate security goals [13].

4. CONCLUSION

In this paper we surveyed the major issues and challenges for cloud computing. We classified the security challenges according to the three cloud service models: SaaS, PaaS, and IaaS. Furthermore, we analyzed existing solutions and provide some direction for how to handle the security threats. There are lots of issues related to security out of which we focused on information security, virtual machine security, and environmental security. We also highlighted the trust, governance and legal issues relevant to cloud computing field. By solving these issues cloud computing can get adequate security and user trust.

REFERENCES

[1] F. Gens. (2009, Feb.). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”, IDC eXchange, Available:

<http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[2] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for Cloud Networking Security", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 68, Part VII, 298-13, DOI: 10.1007/978-3-642-21444-8_26 , SpringerLink, 2015.

[3] N. Provos, M.A. Rajab, P. Mavrommatis," Cybercrime 2.0: When the cloud turns dark", Queue 7(2), PP 46–47 ,2009.

[4] Cloud Computing Architecture edited in 2016 -. Retrieve from http://satimis.com/cloud-computing/

[5] Dan Orlando," Cloud computing service models", 08 Feb 2011 , Retrieve from : www.ibm.com/developerworks/

[6] D. Molnar, S. Schechter, (2010) Self hosting vs. cloud hosting: accounting for the security impact of hosting in the cloud. In: Workshop on the economics of information security.

[7] CSA: Cloud security guide (2009)Tech. rep., cloud security alliance. http://www.cloudsecurityalliance.org/csaguide.pdf

[8] ENISA: Cloud computing: Benefits, risks and recommendations for information security (2009) Techrep., European Network and Information Security Agency.

[9] D. Teneyuca, "Internet cloud security: The illusion of inclusion", Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.005

[10] Minqi Zhou; Rong Zhang; Wei Xie; Weining Qian; Aoying Zhou, "Security and privacy in cloud computing: a survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids, PP 105 – 112, 2010. DOI 10.1109/SKG.2010.19.

[11] PG. Dorey, A. Leite, "Commentary: Cloud computing- A security problem or solution?", Information Security Technical Report (2015), doi:10.1016/j.istr.2011.08.004

[12] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems,elsvier, PP 583-592, 2010, doi:10.1016/j.future.2010.12.006.

[13] Dave Abraham, CEO, Signify, "Why 2FA in the cloud?", Network Security, Volume 2009, Issue 9, PP 4-5, September 2014.

[14] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (2011), PP 1–11. doi:10.1016/j.jnca.2010.07.006

[15] W. Dawoud, I. Takouna, C. Meinel," Infrastructure as a service security: Challenges and solutions", The 7th International Conference on Informatics and Systems (INFOS), PP 1 – 8, 2010.

[16] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance 2015.

[17] B. Hay, K.L. Nance and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", in Proceedings of HICSS, PP 1-7, 2011.

[18] Trilogy Technologies Blog—Thursday 18th June 2015 by John Casey. Retrieve from http://trilogytechnologies.com/top-five-challenges-of-cloud-computing/