ISSN: 2321-7782 (Online)

Volume 2, Issue 5, May 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Paper

Available online at: www.ijarcsms.com

Analogous Study of Security Issues and Challenges in Cloud Environment

Chethan Sharma
Dept of CSE
Christ University
Bangalore

***Abstract:** Cloud computing 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. The main thing that grabs the organizations to adapt the cloud technology is cost reduction through optimized and efficient computing. Cloud Computing provides an efficient and flexible way for services to meet escalating business needs. Cloud-shared infrastructure and associated services make it cost effective alternative to traditional approaches. Perhaps the biggest concerns about cloud computing are security and privacy. The idea of handing over important data to another company worries some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key. In this paper we present a study of different security issues and challenges that could occur in a cloud environment.*

***Keywords:** Cloud computing, security, challenges, risks, threats, vulnerability*

I. INTRODUCTION

A cloud refers to a unique IT environment that is designed for the purpose of remotely provisioning scalable IT resources. This can be achieved by the means of Infrastructure as a Service, Software as a Service and Platform as a Service .With internet access, organizations and individual users can acquire required computing resources, storage space and other services provided by a cloud. It brings great elasticity to the users. As data which may be critical in nature are stored in cloud, users can access their data from anywhere in the world using internet. No infrastructure is needed so no need to worry about disk failures which results in reliability which is the main advantage of the cloud computing. Data can be shared between different users and games can be played with other users of the system. Many companies such as Google, IBM, Amazon, Yahoo and Microsoft are frontrunners in providing cloud computing services. Some organizations such as Rackspace, Facebook, Salesforce, Youtube etc have started to provide all kinds of cloud services through internet in recent times. Currently there are three types of clouds as shown in figure1, public clouds, private clouds and hybrid clouds. Private clouds are internal to an organization which provides services to users who are related to that organization and are not accessible to general public. To endeavour a private cloud project requires a momentous level and intensity of obligation to virtualize the business environment, and requires the organization to re-evaluate decisions about existing resources. Private clouds provide cloud services to very restrictive set of users.

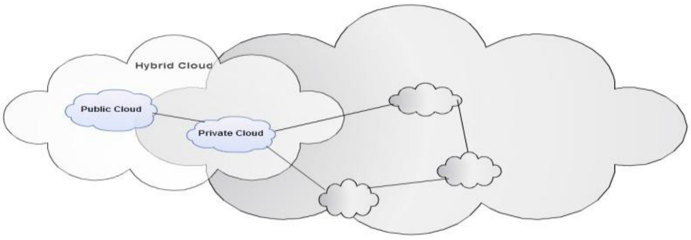
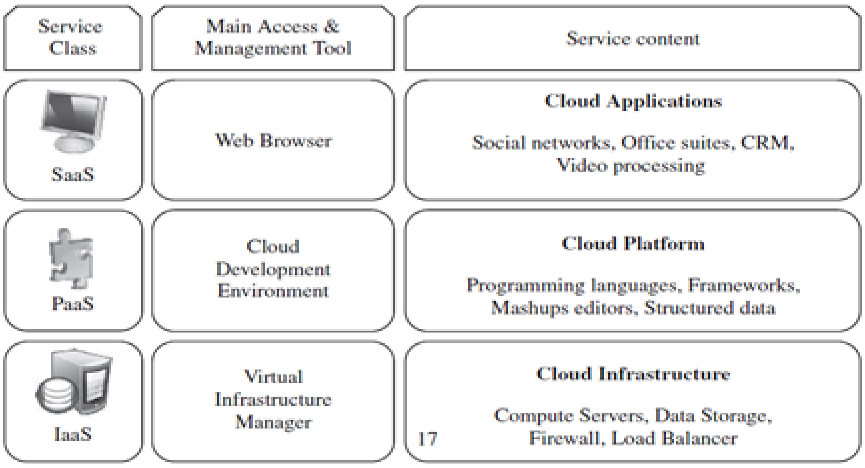


Fig 1. Types of Clouds

Private clouds are internal to an organization which provides services to users who are related to that organization and are not accessible to general public. To endeavor a private cloud project requires a momentous level and intensity of obligation to virtualize the business environment, and requires the organization to re-evaluate decisions about existing resources. Private clouds provide cloud services to very restrictive set of users. Public clouds provide services to general public which includes a large set of users and these clouds can be used by private players to scale-down and scale-up their requirements. Generally, public cloud service providers like Microsoft, Amazon AWS and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered)[1]. Hybrid cloud involves one or more public and/or private clouds [2]. Security in private clouds or public clouds is easier as it consists of a single service provider. In hybrid cloud involving multiple public and private clouds providing security is not as simple as providing security in individual clouds. Service delivery in Cloud Computing comprises three different service models [3], namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).



Service Class	Main Access & Management Tool	Service content
SaaS	Web Browser	**Cloud Applications** Social networks, Office suites, CRM, Video processing
PaaS	Cloud Development Environment	**Cloud Platform** Programming languages, Frameworks, Mashups editors, Structured data
IaaS	Virtual Infrastructure Manager	**Cloud Infrastructure** Compute Servers, Data Storage, Firewall, Load Balancer 17

Fig 2. Cloud Computing Stack [4]

1. *Software as a Service*

SaaS is a way of delivering applications over the Internet—as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management. Since SaaS provides option for paying a monthly fee, it allows organizations to access business functionality at a cost typically less than paying for licensed applications. Cloud users have the authorization to use it for a period of time and pay for the software that they are using. Salesforce.com, which relies on the SaaS model, offers business productivity applications (CRM) that reside completely on their servers, allowing customers to customize and access applications on demand.

Characteristics in Software as a Service are as below [5]

- Network or Online Access
- Centralized Management
- Powerful Communication Features

2. *Infrastructure As A Service*

IaaS is defined as computer infrastructure, such as virtualization, being delivered as a service. Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. IaaS is the virtual delivery of computing resources in the form of hardware, networking, and storage services.

Characteristics in Infrastructure as a Service are as below [4]

- Dynamic scaling
- Advance Reservation of Capacity
- Service-Level Agreement
- Geographic distribution of data centers

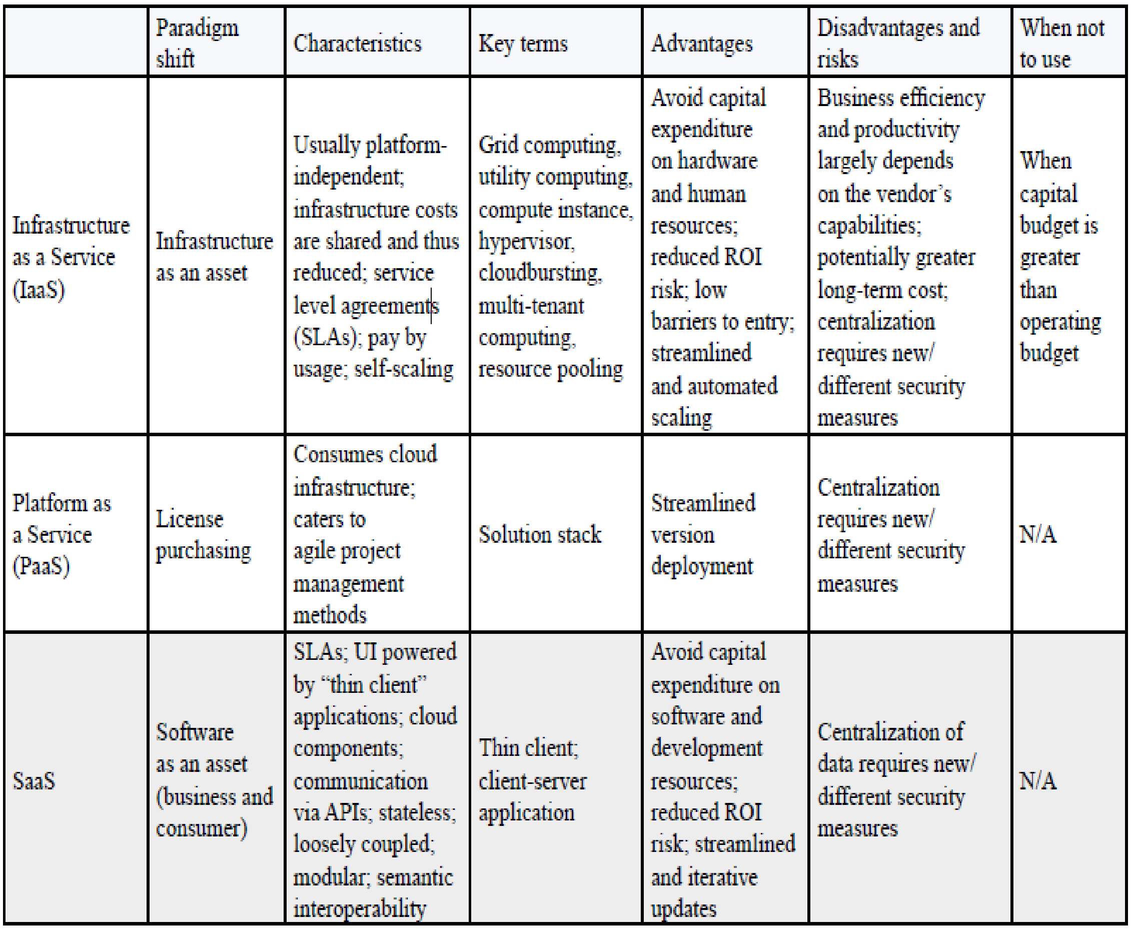
3. *Platform As A Service*

In addition to infrastructure-oriented clouds that provide raw computing and storage services, another approach is to offer a higher level of abstraction to make a cloud easily programmable, known as Platform as a Service (PaaS). A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services are offered as building blocks to new applications. Google AppEngine, an example of PaaS, offers a scalable environment for developing and hosting Web applications, which should be written in specific programming languages such as Python or Java, and use the services' own proprietary structured object data store [4].

Characteristics in Platform as a Service are as below [4]

- Support multiple programming languages.
- Persistence Options
- Minimize operational costs
- Easy collaboration

Following is a brief comparison of Service Models as in [6]



	Paradigm shift	Characteristics	Key terms	Advantages	Disadvantages and risks	When not to use
Infrastructure as a Service (IaaS)	Infrastructure as an asset	Usually platform-independent; infrastructure costs are shared and thus reduced; service level agreements (SLAs); pay by usage; self-scaling	Grid computing, utility computing, compute instance, hypervisor, cloudbursting, multi-tenant computing, resource pooling	Avoid capital expenditure on hardware and human resources; reduced ROI risk; low barriers to entry; streamlined and automated scaling	Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater long-term cost; centralization requires new/ different security measures	When capital budget is greater than operating budget
Platform as a Service (PaaS)	License purchasing	Consumes cloud infrastructure; caters to agile project management methods	Solution stack	Streamlined version deployment	Centralization requires new/ different security measures	N/A
SaaS	Software as an asset (business and consumer)	SLAs; UI powered by "thin client" applications; cloud components; communication via APIs; stateless; loosely coupled; modular; semantic interoperability	Thin client; client-server application	Avoid capital expenditure on software and development resources; reduced ROI risk; streamlined and iterative updates	Centralization of data requires new/ different security measures	N/A

II. SECURITY ISSUES IN CLOUD ENVIRONMENT

IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) are three general models of cloud computing. Each of these models possesses a different impact on application security. However, in a typical scenario where an application is hosted in a cloud, two broad security questions that arise are [7]:

- How secure is the Data?
- How secure is the Code?

Cloud computing environment is generally assumed as a potential cost saver as well as provider of higher service quality. Security, Availability, and Reliability is the major quality concerns of cloud service users. Gens et. al., suggests that security in one of the prominent challenge among all other quality challenges.

The following outlines some of the primary concerns that enterprises should be aware of when planning their cloud computing deployments [7]:

1. *Confidentiality:*

Confidentiality refers to keeping data private. Privacy is of tent amount importance as data leaves the borders of the organization. Not only must internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, among other things, technical tools such as encryption and access control, as well as legal protections.

2. *Assurance:*

Assurance refers to the need for a system to behave as expected. In the cloud context, it is important that the cloud provider provides what the client has specified. This is not simply a matter of the software and hardware behaving as the client expects but that the needs of the organization are understood, and that these needs are accurately translated into information architecture requirements, which are then faithfully implemented in the cloud system. Assurance is supported by a trusted computing architecture in the cloud, and a by careful processes mapping from business case to technical details to legal agreements.

3. *Unencrypted Data:*

Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users [8].

4. *Authentication:*

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. Trusted Computing enables authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

5. *Resilience:*

Resilience in a system allows it to cope with security threats, rather than failing critically. Cloud technology can increase resilience, with a broader base, backup data and systems, and the potential identify threats and dynamically counteract. However, by shifting critical systems and functions to an outside party, organizations can aggravate resilience by introducing a single point of failure. Resilience is supported by redundancy, diversification and real-time forensic capacity.

6. *Virtualization:*

Virtualization is one of the main components of a cloud. Virtual machines are dynamic in nature so that it is difficult to maintain security consistency. Vulnerabilities or configuration errors may be generated easily. The main issue in virtual machine is to keep maintaining the security state for a given time [9] [10].

III. Challenges in Cloud Environment

Following are the few main challenges as per [7]

1. *Administrative Access to Servers and Applications:*

One of the most important characteristics of cloud computing is that it offers “self-service” access to computing power, most likely via the Internet. In traditional data centers, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in system control.

2. *Encryption and Data Protection:*

Many regulations and standards such as the PCI DSS and HIPAA include requirements for the use of encryption to protect critical information—such as cardholder data and personally identifiable information (PII)—to achieve compliance or safe harbour in the event of a breach. The multi-tenant nature of the cloud amplifies these requirements and creates unique challenges with the accessibility and protection of encryption credentials used to ensure data protection.

3. *Data Protection:*

To be considered protected, data from one customer must be properly segregated from that of another; it must be stored securely when “at rest” and it must be able to move securely from one location to another. Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing and/or monitoring cannot be defeated, even by privileged users at the cloud provider.

4. *Availability:*

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

5. *Transparency:*

Security measures assumed in the cloud must be made available to the customers to gain their trust. There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the customers are looking for a different set of security. The important aspect is to see that the cloud provider meets the security requirements of the application and this can be achieved only through 100% transparency.

IV. Conclusion

Cloud computing 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 an efficient and flexible way for services to meet escalating business needs. Cloud-shared infrastructure and associated services make it cost effective alternative to traditional approaches. Perhaps the biggest concerns about cloud computing are security and privacy. In this paper we present a study of different security issues and challenges that could occur in a cloud environment. We also present as brief overview of cloud service models and also compare them. Few security and challenges that could occur in a cloud environment is given.

References

1. http://en.wikipedia.org/wiki/Cloud_computing#cite_note-61
2. IBM Embraces Juniper For Its Smart Hybrid Cloud, Disses Cisco (IBM),http://www.businessinsider.com/2009/2/ ibm embraces-juniper-for-its-smart-hybrid-cloud-disses-cisco-ibm
3. http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/
4. Rajkumar Buyya "Cloud Computing: Principles and Paradigms" ISBN: 978-0-470-88799-8
5. "Cloud computing tutorials" by Exforsys Inc April 12, 2009
6. Sumit Khurana, Anmol Gaurav Verma "Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS" International Journal of Electronics & Communication Technology IJECT Vol. 4, Issue Spl - 3, April - June 2013
7. Dhaval Dave "A Dissertation report on Security in Cloud Computing" Indus Institute of Technology & Engineering ,Gujarat University, 2011
8. Ms. Disha H. Parekh,Dr. R. Sridaran "An Analysis of Security Challenges in Cloud Computing" International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013
9. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy “Cloud Computing: Security Issues and Research Challenges”, International Journal of Computer Science and Information Technology & Security , Vol. 1, No. 2, December 201
10. K.L.Neela Dr.V.Kavitha "A Survey on Security Issues and Vulnerabilities on Cloud Computing" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. 07 Jul 2013.