ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 2, February 2017

# Cloud Computing Security Issues, Challenges and Solution

Prof. Ashok Deokar

Associate Professor, Sinhgad Institute of Management Pune, Savitribai Phule Pune University, Maharashtra, India

**ABSTRACT:** Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. In this paper we have shown Successful implementation of cloud computing in an Organization, enterprise requires proper planning and understanding of emerging risks, fear and possible countermeasures. This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and broadminded steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management. This paper also cover the advantages and disadvantages in the way of cloud computing. This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing.

**KEYWORDS***:* Cloud Computing, Risk, IaaS, PaaS, SaaS, DaaS, Security, Quality Assurance, Threats, Utility Computing,C I A (Confidentiality, Integrity, Availability).

## I. INTRODUCTION

In the increasingly established cloud computing datacenters play a fundamental role as the major cloud infrastructure providers, such as Yahoo, Google, Microsoft Azure, App Point, Cipher Cloud, Wipro, TCS etc. Datacenters provide the utility computing service to software service providers who are further provide the application service to end users through Internet. The later service has long been called as “software as a Service (IaaS)”, where the software service providers is also referred to as a cloud service providers. To take advantage of computing and storage resources provided by cloud infrastructure providers, data owners outsource more and more data to the datacenters through the cloud service providers, e.g., the online storage service provider, which are not fully trusted by data owners.

As general data structure to describe the relation between entities, the graph has been increasingly used to model complicated structures and schema less data, such as the personal social network, the relational data base, for the protection of users privacy , these sensitive data have to be encrypted before outsourcing to the cloud. Moreover, some data are supposed to be shared among trusted partners to all organizations. There have been publicized attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and cloud computing information security management. This paper has discussed some of the services being provided.

## II. CLOUD COMPUTING ARCHITECTURE

There are several major cloud computing providers including Infosys, Amazon Azure, TCS, Google, Yahoo, Wipro, Microsoft and others that are providing cloud computing services (Figure1. shows current cloud providers). Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, Desktop-as-a-services (DaaS), Software-as-a-services (SaaS), Infrastructure-as-a-services (IaaS) and Platform-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

as-a-services (PaaS).

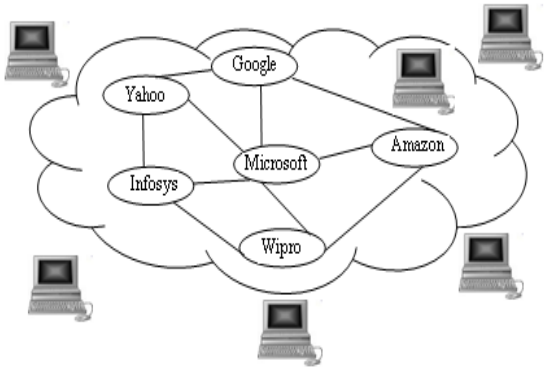


**Figure-1 Cloud Computing Architecture**

The attractiveness of cloud computing is not only to large enterprises but also entrepreneurs, startups, medium scale companies and small scale companies would benefit greatly and they will have a new alternative and opportunities that is not available to them in the past that would save them millions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, storage space and communication capacity from a large cloud computing provider that has all of these assets connected to the Internet**.** In practice, cloud service providers tend to offer services that can be grouped into four categories: software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS) and Desktop as a Service (DaaS).These categories group together the various layers illustrated in Figure2, with some overlap.

***A. Desktop as a Service (DaaS)***

If you want to provide applications, content, and data anytime, anywhere, on any device. You also want to simplify desktop operations, improve security, manage costs, and help the business. Desktop virtualization provides a high-quality user experience while managing security and total cost of ownership. Desktop as a service (DaaS) allows you to enjoy the many benefits of desktop virtualization without having to acquire, build, and manage your own infrastructure.

***B. Software as a Service (SaaS)***

If provide software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

***C. Infrastructure as a service (IaaS)***

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications. Commercial examples of IaaS include Joyent, whose main product is a line of virtualized servers that provide a highly available on-demand infrastructure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

### *D. Platform as a service (PaaS)*

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services:


**Figure 2 Cloud Services and Application**

Someone producing PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service. For example, someone developing a PaaS offering might base it on a set of Sun™ xVM hypervisor virtual machines that include a NetBeans™ integrated development environment, a Sun GlassFish™ Web stack and support for additional programming languages such as Perl or Ruby.

Someone using PaaS would see an encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale itself to provide a given level of service. Virtual appliances can be classified as instances of PaaS. A content switch appliance, for example, would have all of its component software hidden from the customer, and only an API or GUI for configuring and deploying the service provided to them. PaaS offerings can provide for every phase of software development and testing, or they can be specialized around a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google's infrastructure. PaaS services such as these can provide a powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

## III. THREATS IN CLOUD COMPUTING

### *A. THREATS*

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

***Following major threats:***

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems.
- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities.
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

## IV. CLOUD COMPUTATION IMPLEMENTATION GUIDELINES

### *A. STEPS TO CLOUD SECURITY*

Edwards (2009) stated that, with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider:

- ***Understand*** the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.

- ***Demand*** *Transparency* by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.

- ***Reinforce Internal Security*** by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.

- ***Consider the Legal Implications*** by knowing how the laws and regulations will affect, what you send into the cloud.

- ***Pay attention*** by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

### *B. INFORMATION SECURITY PRINCIPLES*

*C I A (Confidentiality, Integrity, Availability)*

• *Confidentiality*

Prevent unauthorized disclosure

• *Integrity*

Preserve information integrity

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

• *Availability*
Ensure information is available when needed

### *C. IDENTIFY ASSETS & PRINCIPLES*

- *Customer Data*
  Confidentiality, integrity, and availability.
- *Customer Applications*
  Confidentiality, integrity, and availability.
- *Client Computing Devices*
  Confidentiality, integrity, and availability.

## V. ISSUES TO CLARIFY BEFORE ACCEPTING CLOUD COMPUTING

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

• ***User Access***. Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.
• ***Regulatory Compliance***. Make sure your provider is willing to submit to external Audits and security certifications.
• ***Data location***. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.
• ***Data Segregation***. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.
• ***Disaster Recovery Verification.*** Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.
• ***Disaster Recovery***. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.
• ***Long-term Viability***. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

## VI. SOLUTION OF SECURITY ISSUES

### *A. FIND KEY CLOUD PROVIDER*

First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

### *B. CLEAR CONTRACT*

Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

### *C. RECOVERY FACILITIES*

Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

### *D. BETTER ENTERPRISE INFRASTRUCTURE*

Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

### *E. USE OF DATA ENCRYPTION FOR SECURITY PURPOSE*

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor.

IT leaders must define strategy and key security elements to know where the data encryption is needed.

### *F. PREPARE CHART REGARDING DATA FLOW*

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

## VII. CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

## REFERENCES

[1] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.
[2] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM ; 2010; 53(4):50–58.
[3] Subashini S, Kavitha V. A survey on security i ssues in service delivery models of cloud computing. Journal of Network and mputer Applications; 2011; 4(1):1–11.
[4] Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.
[5] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyz ing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54 :255–265.
[6] Boss G, Malladi P, Quan D, Legre gni L, Hall H. Cloud computing,2009. http://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.
[7] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing(Draft). NIST. 2011. http://www.productionscale.com/home/2011/8/7/the-nist-definition-of-cloud-computingdraft.html#axz z1X0xKZRuf.
[8] Cloud Security Alliance. Security gui dance for critical areas of focus in cloud computing(v2.1). Decemeber, 2009.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

**Vol. 5, Issue 2, February 2017**

[9] Pearson, S. and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing" in 2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom),Nov 30-Dec 3,2010, page(s): 693-702.
[10] Jinzhu Kong, "A Practical Approach to Improve the Data Privacy of Virtual Machines" 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), June 29 -July 1 ,2010, pp. 936-941.
[11] Esteves, R.M. and Chunming Rong, "Social Impact of Privacy in Cloud Computing" in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), N ov. 30-Dec. 3 ,2010, pp. 593-596
[12] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller
[13] Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.
[14] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe
[15] Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar
[16] Ramanujam, S., Gupta, A., Khan, L., & Seida, S(2009). R2D: Extracting relational structure from RDF stores. In Proceedings of the ACM/IEEE International Conference on Web Intelligence, Milan, Italy
[17] Smith, S., & Weingart, S. (1999). Building a high performance, programmable secure coprocessor [Special Issue on Computer Network Security]Computer Networks, 31, 831–860. doi:10.1016 S1389-1286(98)00019-X
[18] Teswanich, W., & Chittayasothorn, S. (2007). ATransformation of RDF Documents and Schemascto Relational Databases. IEEE Pacific Rim Conferences on Communications, Computers, and Signal Processing, 38-41.
[19] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012)