April - June © 2018 Transactions; 5(18): 816-819

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Case Study

Cloud security - A current scenario and characteristics of cloud computing

Sudheer Kumar Shriramoju

Corresponding Author:
sudheerpapers@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.5.18 (4)2018

Manuscript:
Received: 22nd Apr, 2018
Accepted: 17th May, 2018
Published: 27th June, 2018

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Cloud computing is expressively leading today's IT enterprises towards achieving their business goals alongside providing utmost customer satisfaction with very lower cost with respect to infrastructure, platforms, and software perspectives. While these infrastructure-related hassles handled by a CSP, cloud service provider, organization needs to completely focus on the service to their customers. Being a user of cloud services from CSP, organizations need not have high technical potential with respect infrastructure and platforms. Whereas, Cloud Service Users need to have expertise on the functionality provisioning/servicing based on their customer requirements. Alongside to its benefits, cloud computing is also comes with various challenges. Among all, security being a leading threat. This paper provides the current scenario of cloud security.

Keywords: Cloud computing, architecture, characteristics.

Project Manager, Wipro InfoTech, Hyderabad, India.

IJRA - Year of 2018 Transactions:
Month: April - June
Volume – 5, Issue – 18, Page No's:816-819
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2018: 5(18)816-819

DOI: 10.17812/IJRA.5.18(4)2018

International Journal of Research and Applications
Apr - Jun © 2018 Transactions 5(18): 816-819

eISSN : 2349 – 0020
pISSN : 2394 – 4544
www.ijraonline.com

COMPUTERS CASE STUDY

Cloud security - A current scenario and characteristics of cloud computing

Sudheer Kumar Shriramoju
Project Manager, Wipro InfoTech, Hyderabad, India.
sudheerpapers@gmail.com

ABSTRACT

Cloud computing is expressively leading today's IT enterprises towards achieving their business goals alongside providing utmost customer satisfaction with very lower cost with respect to infrastructure, platforms, and software perspectives. While these infrastructure-related hassles handled by a CSP, cloud service provider, organization needs to completely focus on the service to their customers. Being a user of cloud services from CSP, organizations need not have high technical potential with respect infrastructure and platforms. Whereas, Cloud Service Users need to have expertise on the functionality provisioning/servicing based on their customer requirements. Alongside to its benefits, cloud computing is also comes with various challenges. Among all, security being a leading threat. This paper provides the current scenario of cloud security.

Keywords: cloud computing, architecture, characteristics.

1. INTRODUCTION

Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user.

Figure 1: Cloud Computing

Some generic examples include:

- Amazon's Elastic Computing Cloud (EC2) offering computational services that enable people to use CPU cycles without buying more computers.
- Storage services such as those provided by Amazon's Simple Storage Service (S3).
- Companies like Nirvanix allowing organizations to store data and documents without adding a single on-site server.
- SaaS companies like Salesforce.com delivering CRM services, so clients can manage customer information without installing specialized software.

SOFTWARE AS A SERVICE (SAAS)

SaaS is a model of software deployment where an application is hosted as a service provided to customers across the Internet. SAAS is generally used to refer to business software rather than consumer software, which falls under Web 2.0. By removing the need to install and run an application on a user's own computer it is seen as a way for businesses to get the same benefits as commercial software with smaller cost outlay. SaaS can alleviate the burden of software maintenance and

support but users relinquish control over software versions and requirements. Other terms that are used in this sphere include *Platform as a Service* (PaaS) and *Infrastructure as a Service* (IaaS).

CLOUD STORAGE

Over time many big Internet based companies (Amazon, Google…) have come to realize that only a small amount of their data storage capacity is being used. This has led to the renting out of space and the storage of information on remote servers or "clouds". Information is then temporarily cached on desktop computers, mobile phones or other internet-linked devices. Amazon's Amazon Elastic Compute Cloud (EC2) and Simple Storage Solution (S3) are the current best known facilities.

DATA CLOUD

Along with services the cloud will host data. There has been some discussion of this being a potentially useful notion possibly aligned with the Semantic Web, though it could result in data becoming undifferentiated.

2. CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing, typically entails:

High scalability
Cloud environments enable servicing of business requirements for larger audiences, through high scalability.

Agility
The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).

High availability and reliability
Availability of servers is high and more reliable as the chances of infrastructure failure are minimal.

Services in pay-per-use mode
SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.

Support for all service oriented applications

3. CLOUD ARCHITECTURE

Cloud Architectural Models
The term cloud architecture or cloud computing architecture indicates the components and sub components which are required to implement a well-defined and efficient cloud computing set up. The architecture consists of a front end platform, back end platform, a cloud based delivery and a network. These components also consist of sub components that together make up cloud computing architecture. The front end platform consist of fat client, thin client and mobile devices. The back end platforms include servers and storage. The architecture component network consists of an Internet or intranet.

- Front End Platforms
- Back End Platforms
- Cloud Based Delivery
- Cloud Networking

Advantages of Cloud Computing in the Current Scenario

- Cost Efficient
- Flexibility of Work Practices
- Collaboration Efficiency
- Access to Automatic Updates
- Reliability
- Scalability
- Business Continuity
- Innovation
- Multiple Users at One Time
- Customize Settings

4. PROBLEMS IN CLOUD COMPUTING

Cloud computing attracts users with its great elasticity and scalability of resources with an attractive tag line 'pay-as-you-use' at relatively low prices. Compared to the construction of their own infrastructures, customers are able to cut down on expenditure significantly by migrating computation, storage and hosting onto the cloud. Although this provides savings in terms of finance and manpower, it brings lots of new challenges and risks. Considering the influence of cloud computing with respect to its business benefits and technological transformations, the future enterprise applications are going to be completely dependent on it. It has its own benefits; nevertheless it has numerous issues and challenges.

- Data Integrity
- Data Theft

- Privacy Issues
- Infected Application
- Data Loss
- Data Location
- Security on Vendor Level

5. CLOUD SECURITY – A CURRENT SCENARIO

Security Scenarios

Cloud computing is a well-known technology nowadays. Companies like Amazon, Google and Microsoft are enhancing the services provided for their users. Security issue is a barrier for users to adapt into cloud systems. Cloud service providers have been concerned of the non-adequate security measures and aspects like data integrity, control, audit, confidentiality, availability should be added. Privacy acts which are in use are out of date and are not protecting the private information of user in the cloud environment since they are not applicable to three parties like cloud service user, cloud service provider, cloud provider. Privacy issue becomes worse when applications are in multiple locations. Cloud computing offers storage of data with scalable power of processing that elevated IT to newer limits with low capital expenditure. If one runs the application in public domain or beyond firewall then there arises security consciousness and concerns.

In cloud computing the consumers can access resources online at any time through Internet without managing the original resources issues like physical and technical management. Cloud computing resources are scalable and dynamic. The significant difference in cloud security is enterprise control loss opposed to particular technical challenge. In cloud based application access control is important. The application of security, infrastructure and platform is under provider's control.

Regulations

It determines the functional requirements of security and not the technical issues. Other than technical issues in cloud computing, regulations is the harsh reality. The governments are concerned about the cloud computing for many reasons. The privacy laws are followed by many countries that prohibit the data which stores on physical machine located outside the country. The organizations are penalized for violating laws. In cloud if any organization stores sensitive data then the cloud provider should prove that it never stores data outside geographical area. Other than government agencies trade and industry groups create regulations. That regulation represents best practices.

It is applicable to the applications which are running in the cloud. An application which is running on the virtual machine can access the sensitive data or not, this is not addressed by many countries. A new law is required for an organization to spend the resources which changes the application infrastructure than adding features to it.

Security Controls

Consumer needs all security controls which should not vary based on cloud provider that makes claims on security related issues and reassurances. For a secure system a number of controls are necessary.

Security Control Descriptions:

Asset Management: To manage the hardware, network and software assets which make up the cloud infrastructure. This includes physical access of asset for audit.

Cryptography (Key and Certificate Management): Infrastructure for managing cryptographic keys are needed for a secure system. It includes employing cryptographic functions and services for information security.

Data Security: The data is to be stored in encrypted format. The data of one consumer should be separated from other consumer.

Endpoint Security: Consumers must secure the endpoints to the resources in the cloud. It includes restricted endpoints by device type and network protocol.

Event Auditing and Reporting: Consumers must be able to access data about events happened in the cloud, especially security breaches and system failures. The access event includes the learning of past events and new events reporting. Cloud providers cause damage to their reputations when they fail in reporting events timely.

Identity, Roles, Access Control and Attributes: It must be possible to define the entitlements,

identity, roles and individual attributes and services in a machine-readable way and consistent in order to implement access control effectively and enforce security policy.

Network Security: It must be possible to secure network traffic at the router, switch and packet level. The IP stack also should be secure.

Security Policies: It must be possible to resolve, define policies and enforce policies of security in support of access control, resource allocation and other decisions in a machine readable and consistent way.

6. CONCLUSION

This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization. This paper provided the current scenario of cloud security.

REFERENCES

1) S. Watson. (Mar. 1, 2010). HP, Cloud Security Alliance Identify Top Cloud Security Risks. .
2) D. Ohara. (Oct. 11, 2009). Cloud Computing PR disaster - Failure Sinks the Server in Microsoft/Danger's Client/Server Model – Client Data unrecoverable. [On-line]. GreenM3. Available: http://www.greenm3.com/gdcblog/2009/10/11/cloud-computing-pr-disaster-failure- sinks-the-server-in-micr.html.
3) G. Lawton. (Jan. 2010). What's in store for cloud computing in 2010? [On-line]. Available: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1378037,00.html
4) L. Whitney. (Dec. 11, 2009). Amazon EC2 cloud server hit by botnet outage. [On-line]. Cnet News. Available: http://news.cnet.com/8301-1009_3-10413951-83.html.
5) "Epsilon Data Breach Hits Major Brands", Puget Sound Business Journal (Seattle, WA), Apr. 4, 2011.
6) Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.
7) Sudheer Kumar Shriramoju, "Review on NoSQL Databases and Key Advantages of Sharepoint", International Journal of Innovative Research in Science, Engineering and Technology, ISSN (Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, and November 2018.
8) Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint on Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 2, Issue 6, November-December-2017.
9) Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016.
10) Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014.
11) Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012.
12) Sudheer Kumar Shriramoju, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013.