International Journal of Grid Distribution Computing
Vol. 8, No.5, (2015), pp.215-222
http://dx.doi.org/10.14257/ijgdc.2015.8.5.21

A Review of Cloud Computing Security Issues

[1]Manpreet Kaur and [2]Hardeep Singh

[1]Research Fellow, Chandigarh Group of College, Landran
Cutemani.shergill@gmail.com
[2]Asst. Professor, Chandigarh Group of College, Landran
Cgccoe.cse.hardeep@gmail.com

Abstract

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud computing stores the data and its disseminated resources in the environment, security has become the main obstacle which is hampering the deployment of cloud environments. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party. The importance of third party is to prevent and control unauthorized access to data store to the cloud. This research paper discusses the security issues of cloud storage.

Keywords: *Cloud computing, cloud data storage, cloud data security, Deployment models, Service models, cloud security challenges*

1. Introduction

The term "Cloud Computing" is the computing services in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet. Infrastructure upon which cloud is built upon is a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Hence it can be easily concluded that according to the requirements and current workloads, the services of cloud could be scaled dynamically. As many resources are used, they are measured and then the payment is made on the basis of consumption of those resources.

According to the definition of[10], cloud computing is "it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet". There are some examples of cloud services like webmail, online file and business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage [13] specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. The mechanism [13] model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform. The basic cloud storage environment represented as below:

ISSN: 2005-4262 IJGDC
Copyright ⓒ 2015 SERSC

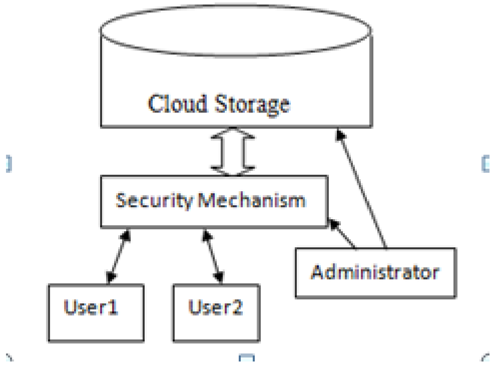

Figure 1. Cloud Storage Environment

2. Cloud Services Models

Cloud Infrastructure as a Service (IaaS): In this composition of implemented environment for their system a supplier must be supply different computing resources which include loading, processing unit. Client has flexile to achieve and switches software mutilated to be implemented and vary between different applications like operating system etc. There are different issues in IaaS such as:

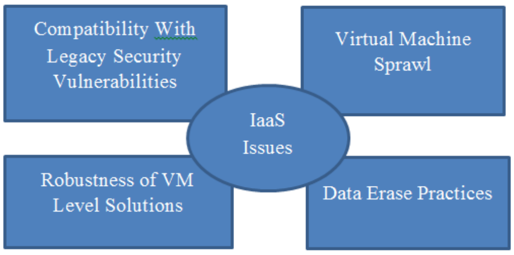
Compatibility With Legacy Security Vulnerabilities
Virtual Machine Sprawl
IaaS Issues
Robustness of VM Level Solutions
Data Erase Practices

Figure 2. IaaS Issues

Cloud Platform as a Service (PaaS): This software supplies client with the ability to establish and extended applications that are mainly positioned on equipment and programming languages promoted by the suppliers. In this the client has no containment over the different organization but has containment over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space. There are different issues in PaaS such as:

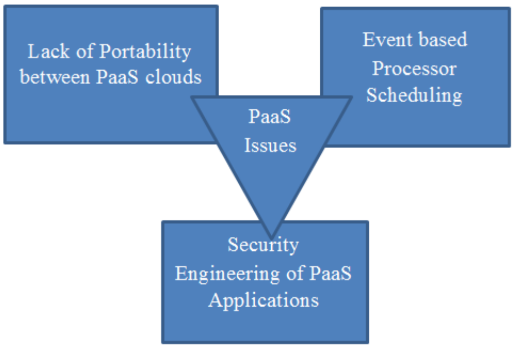
Lack of Portability between PaaS clouds
Event based Processor Scheduling
PaaS Issues
Security Engineering of PaaS Applications

Figure 3. PaaS Issues

Copyright ⓒ 2015 SERSC

Types of PaaS: There are different types of PaaS such as

- Application Delivers only Environments
- Standalone Developments Environments
- Open Platform & Open Service
- Add on Development Possibility

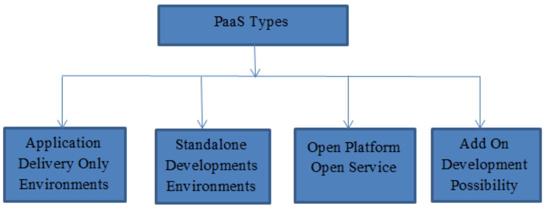
PaaS Types
Application Delivery Only Environments
Standalone Developments Environments
Open Platform Open Service
Add On Development Possibility

Figure 4. PaaS Types

Cloud Software as a Service (SaaS): This software supplies the ability to usage the appliances which implemented on cloud organization. With the usage of standard interfaces like web browser or online (e-mail) client, these appliances are obtainable. SaaS appliances are obtained from different devices like mobile, workstation from anywhere at any time.

Cloud Network as a Service (NaaS): NaaS provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network.

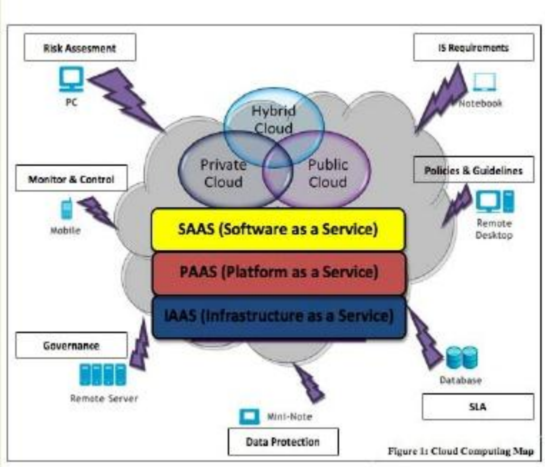

Figure 5. Cloud Computing Map [5]

3. Cloud Deployment Models

Public Cloud: Public cloud describes the conventional meaning of cloud computing that is accessible, effective ways and means, which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility. Cloud organization is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model. The following figure shows some of those benefits:

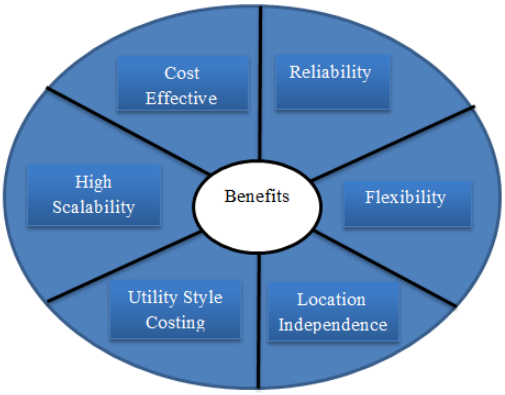

Figure 6. Benefits of Public Cloud

Private Cloud: Private cloud is a term used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house ‘service providers’ catering to customers within the corporation. Cloud organization is establishing for a particular aggregation and managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are advantages (benefits) of internal cloud model. The diagram given below depicts a few of these advantages (benefits):

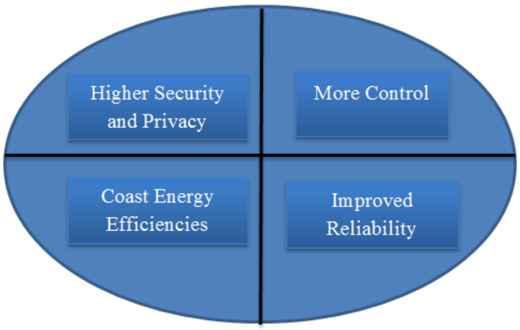

Figure 7. Benefits of Private Cloud

Hybrid Cloud: A hybrid cloud comprises assets from both corporate and public providers will definitely become the demanded choice for enterprises. The hybrid cloud is a combination of both corporate cloud and public cloud.. For example, for general computing enterprise could selects to make usage of external services, and its own data Centre’s comprises it own data Centre’s. Hybrid cloud model has number of advantages (benefits).The diagram given below reveals some of those advantages (benefits):

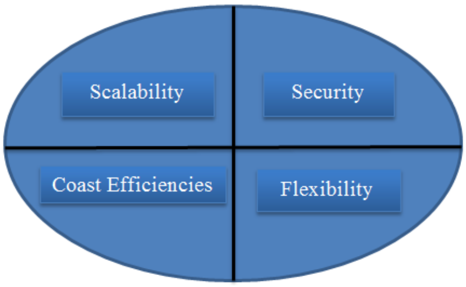

Figure 8. Benefits of Hybrid Cloud

Copyright ⓒ 2015 SERSC

4. Cloud Computing Characteristics

On Demand Self-Service: A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.

Broad Network Access: Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.

Resource Pooling: A multitudinous model is employed to serve different types of clients by making pools of different computing resources, as per the request of customers these have different resources which can be assigned and reassigned dynamically.

Rapid Elasticity: Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities come out to be limitless and must have the capability to purchase in any quantity at any time.

Measured Services: The provision procured by different clients is measurable, The use of asset will be directed, estimated, and accused for contributor and asset.

5. Cloud Security Challenges

There are some key security [5] challenges are:

Authentication: Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have interchangeability administration entity.

Access Control: To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA).

Policy Integration: There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches.

Service Management: In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procuring divider to get the easiest localized services.

Trust Management: The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider.

6. Security Feature in Cloud Computing

There are several main challenges for building a secure band trustworthy cloud system:

Outsourcing: Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owner's control.

Massive data and intense computation: Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

7. Security Issues

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), and Infrastructure as a service (IaaS). Each service has their own security issues [3]

Data Security: Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of data. Confidentiality is designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Availability is defined as data is available on time.

Regulatory Compliance: Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification, Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations [11].

Data Locations: When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement [9].

Privileged User Access: Outside the resource data that is processed contains an indigenous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

Trust Issue: Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

Data Recovery: It is defined as the process of restoring data that has been lost, corrupted or accident.

8. Conclusion & Future work

Cloud computing is latest technology that is being widely used all over the world. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography. Number of cloud platforms are available now in educational as well as in enterprises circle

In this paper, we have discussed the issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has bright future.

References

[1] A. Boldreva, N. Chenette, Y. Lee and A. O'neill, "Order-preserving Symmetric encryption", Advances in Cryptology-EUROCRYPT 2009 Springer, Berlin/Heidelberg, **(2009)**, pp. 224-241.

[2] D. Boneh, G. Di, R. Ostrovsky and G. Persiano, "Public key encryption with keyword search", Advances in Cryptology-Eurocrypt, Springer, Berlin/Heidelberg, **(2004)**, pp. 506–522.

[3] B. R. kandukuri, R. V. Paturi and A. Rakshit, "Cloud security issues", IEEE International Conference on Services Computing, Bangalore, India, **(2009)** September 21-25, pp. 517-520.

[4] J. Campbell, "Applied Virtualization Technology," Hillsboro, Intel Press (ISBN 0

[5] 9764832-3-8), **(2006)**, pp. 69-73.

[6] R. Chandrahasan, S. Kalaichelvi, S. Priya and L. Arockiam, "Research Challenges and Security Issues in Cloud Computing", International Journal of Computational Intelligence and Information Security 3.3, **(2012)**, pp. 42-48.

[7] C. –T. Huang, Z. Qin and C. -C. J. Kuo, "Multimedia Storage Security in Cloud Computing, an Overview" 978-1-457701434- 4/11/$26.00,IEEE, **(2011)**.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing v1.0," Prepared by the Cloud Security Alliance, **(2010)** March, pp. 1-14.

[9] D. Xin, *et al*., "achieving secure and efficient data collaboration in cloud computing", Quality of service, 2013 IEEE/ACM 21st International symposium on.IEEE, **(2013)**.

[10] F. –T. Lin, T. –S. Shih, "Cloud Computing: The Emerging Computing Technology", ICIC Express Letters Part B: Applications (ISSN: 2185-2766), vol. 1, **(2010)** September, pp. 33-38.

[11] I. T. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared CoRR", abs/0901.0131 **(2009)**.

[12] G. Hughes, D. Al-Jumeily and A. Hussain, "Supporting Cloud Computing Management through an Object Mapping Declarative Language" Developments in E-Systems engineering **(2010)**.

[13] J. Mäenpää, "Cloud Computing with the Azure Platform", TKK T-110.5190 Seminar on Internet Working, **(2009)** April 27.

[14] D. K. Chander and Y. Sharma, "Enhanced Security Architecture for Cloud Data Security", International Journal of Advanced Research in Computer Science and Software Engineering 3.5, **(2013)**, pp. 571-575.

[15] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing and Emerging IT Platforms, Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer System, **(2009)**, pp. 599-616.

[16] K. Ren, C. Wang and Q. Wang, "Security challenges for the public cloud". IEEE Internet Comput vol. 16, no.1, **(2012)**, pp. 69–73.

[17] S. Tout and Lawver, "Cloud Computing and its Security in Higher Education," In Proceedings of the Proc ISECON **(2009)**.

[18] M. Vaquero and Lindner, "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, vol. 39 no. 1, **(2009)** January, pp. 50-55.

[19] W. Zeng, Y. Zhao, K. Ou and W. Song, "Research on cloud storage architecture and key technologies", in Proceedings of the 2nd International Conference on Interaction Sciences, Information Technology, Culture and Human, Seoul, Korea, **(2009)**, pp. 1044-1048.

[20] Z. Xia, Y. Zhu, X. Sun and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking", Journal of Cloud Computing, Springer, vol. 3, no. 1, **(2009)**, pp. 1-11.

[21] Y. Ye, L. Xiao, I. –L. Yen, F. Bastani, "Secure, Dependable, and High Performance Cloud Storage", 29th IEEE International Symposium on Reliable **(2009)**.

Authors

Manpreet kaur, she is pursuing her Masters in computer science and engineering from Chandigarh Group of college (CGC-COE) Landran, Mohali, (Punjab). She received the bachelor of technology degree from BGIET, Sangrur. Her research interests are lies in the field of Cloud Computing. Her current research work is based on the security issues in cloud computing.

Hardeep Singh, he works as assistant professor in CGC-COE landran Mohali, Punjab. He gives the guidance in this paper. He has completed his masters in computer science & engineering from Baba Banda Singh Bahadur College, Fatehgarh sahib. His research interest are in the fields of software engineering, cloud computing, cyber administration.

Copyright ⓒ 2015 SERSC