ISSN: 2321-7782 (Online)
Volume 3, Issue 7, July 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

CLOUD: Architecture, Security Threats Issues and Countermeasures for Security

Shewta Chandage[1]
ME CSE Scholar
Department of Computer Science & Engineering
Anuradha Engineering College, Chikhli, (MS)
India

Vishal S. Patil[2]
Asst. Professor
Department of Computer Science & Engineering
Anuradha Engineering College, Chikhli, (MS)
India

Abstract: ***Cloud computing is a model of providing on demand, convenient and continuous network access to shared pool of computing resources. Cloud computing is an internet based computing where shared resources and information is available to access for every service users on demand. It is an efficient way to access share distributed resources and services those belongs to different workstations of different organizations. Security issues in cloud are major active area of research because of many security threats that are currently present. 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 mainly focuses on security threats of cloud computing system also provide some solutions and countermeasures on these security problems***

Keywords: Cloud, Cloud Security, Security issues, Security Challenges, Security Countermeasures.

I. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts [1]. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [2]. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [3] [4]. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment.

In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities [5].Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google, ibm, salesforce, zoho, rackspace, Microsoft. It also shares necessary software's and on-demand tools for various IT Industries. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises [6].

II. BLOCKS IN CLOUD COMPUTING

The architecture of the Cloud mainly involves multiple cloud components interacting with each other for the various information they holds on too, thus helping the user to get to the required data on a faster rate as compared to dedicated client-server architecture. When it comes to cloud computing architecture it is mainly based upon the frontend and the back end. The frontend is the Client or information user who requires the data, whereas the backend is the numerous data storage device also known as server which builds the Cloud [6].

© 2015, IJARCSMS All Rights Reserved

There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Private cloud provides better control and more flexibility. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries. The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy [6].

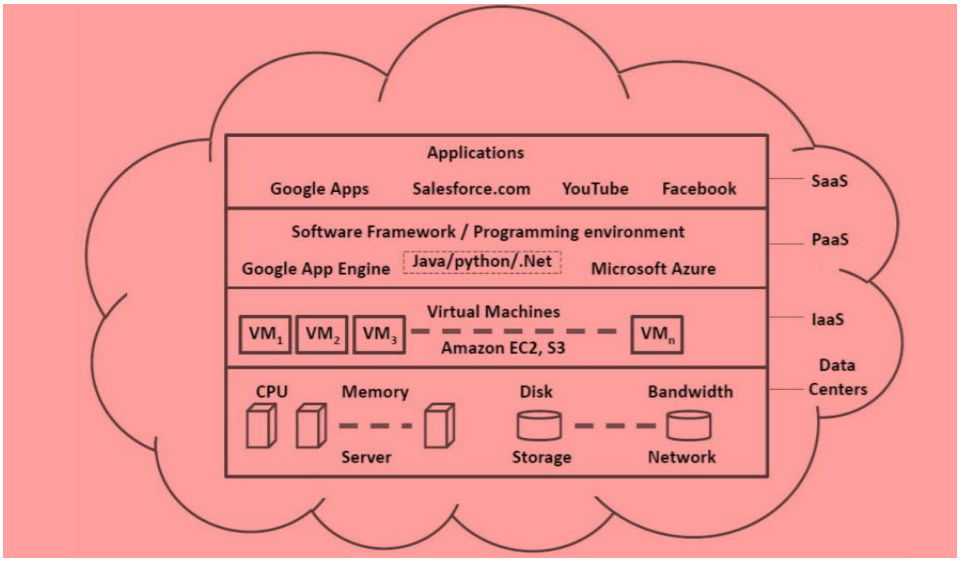

Fig 1: Cloud Computing Architecture

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

a) Software-as-a-Service (SaaS):

SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support [7]. Examples of SaaS includes: Salesforce.com, Google Apps.

b) Platform as a Service (PaaS):

"PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

c) Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. Examples of IaaS include Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

There are also different cloud deployment models namely Private clouds, Public cloud, and Hybrid cloud.

© 2015, IJARCSMS All Rights Reserved

a) Private cloud:

Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems [8].

b) Public Cloud:

A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.

c) Hybrid Cloud:

A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [9]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution.

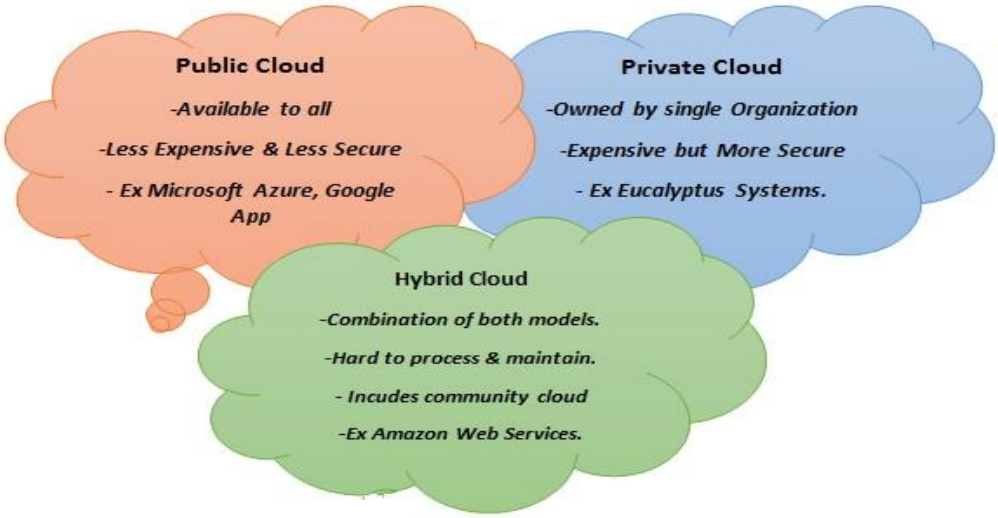

Fig 2: Cloud Deployment Model

III. Security Issues in Cloud Computing

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [8].

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in

© 2015, IJARCSMS All Rights Reserved

several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud [7]. There are four types of issues raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues

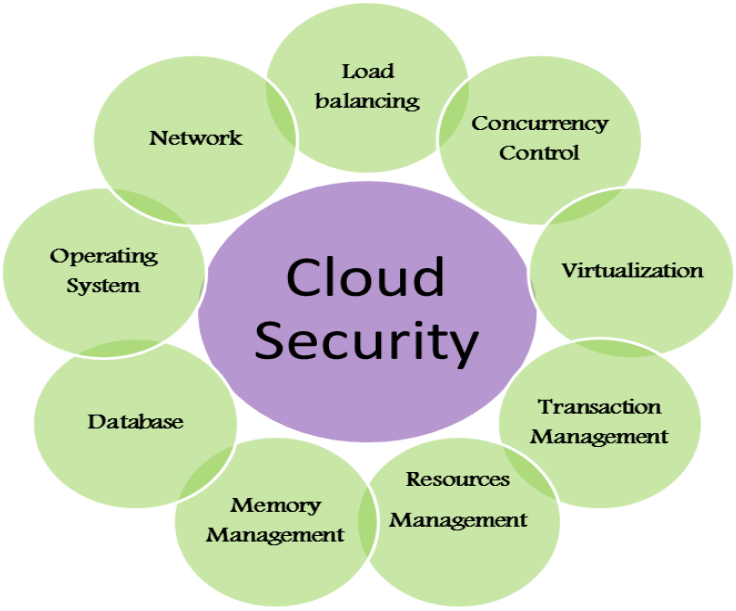

Fig 3: Parameters Affecting Cloud Security

1. Data Issues:

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accesses able to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

© 2015, IJARCSMS All Rights Reserved

2. Privacy Issues:

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

3. Infected Application:

Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

4. Security issues:

Cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

IV. COUNTERMEASURES ON CLOUD SECURITY THREAT

There are some cloud security solutions, that providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution. Trust between the Service provider and the customer is one of the main issues cloud computing. Service Level Agreement (SLA) is the only legal document between the customer and service provider. Which contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do.

Legal Issues is also one of the major problems, the laws vary from country to country, and users have no control over where their data is physically located. Regulatory measures likes, privacy laws and data security laws that cloud systems need to follow. Preserving confidentiality and Integrity is one of the major issues. Data encryption preventing the improper disclosure of information. Authenticity may vary with varying amount of users rights. Sometimes there would be a user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete Solution for such problems is to use digital signatures. Then the problem with digital signatures is that not all users have access to the data superset, therefore they cannot verify any subset of the data even if they're provided with the digital signature of the superset; and too many possible subsets of data exist to create digital signatures for each. Solutions to this problem are to provide customers with the superset's signature and some metadata (verification objects) along with the query results [11]. Data Splitting is also a solution for cloud security issues. Here the data split over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original.

Data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data. Make sure the consumer's access devices or points such as personal computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. Access to the device by an unauthorized user can cancel even the best security protocols loss of an endpoint access device in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features. Data Access Monitoring have to assure about whom, when and what data is being accessed for what purpose. Cloud service provider must share diagrams or any other information or provide audit records to the consumer

© 2015, IJARCSMS All Rights Reserved

or user. Provider must verify the proper deletion of data from shared or reused devices. Cloud service providers must give enough details about fulfilment of promises, break remediation and reporting contingency [12].

V. CONCLUSION

Sharing resources is one of the most worries in providing security in cloud computing platform. Every cloud vendor must inform their cloud sharing customer about the security policies used on their cloud. In this paper, we first discussed about various blocks present in cloud architecture also various deployment model then security issues and research challenges in cloud computing and also various countermeasures available to deal with these security thefts. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud architecture, it will be difficult to achieve total end-to-end security because as the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the cloud computing blocks, model security parameters in cloud structure also some provided countermeasures may be consider for further research work.

References

1. Michael glas and paul Andres, "An Oracle white paper in enterprise architectureachieving the cloud computing vision", CA-U.S.A, Oct 2010.
2. Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.
3. Dr. Gurdev Singh, Shanu Sood, Amit Sharma, "CM- Measurement Facets for Cloud Performance", IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.
4. Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST, Germany.
5. Tackle your client's security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues-withcloud-computing-in-10-steps.
6. Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.
7. R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
8. B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on ServicesComputing, pp. 517-520, 2009.
9. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.
10. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51,University of Texas, USA,April-June 2010.
11. Joshua Kissoon, Cloud Computing Security Issues and Solutions, 2013 Gountis and A. G. Bakirtzis, "Bidding strategies for electricity producers in a competitive electricity marketplace," IEEE Trans. Power System, vol. 19, no. 1, pp. 356–365, Feb. 2004.
12. Anitha Y "Security Issues in Cloud Computing - A Review" , International Journal of Thesis Project and Dissertation , Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013, Available At: www.researchpublish.com

AUTHOR(S) PROFILE

Miss. Shewta S. Chandage, ME CSE Scholar in the Department of Computer Science & Engineering. Received Bachelor's Degree in Information & Technology from SGBAU Amravati University in 2013.

Mr. Vishal S. Patil, received the ME degree in Computer Science & Engineering from SGBAU Amravati University in 2014. Currently working as Asst. Professor in Anuradha Engineering College, Chikhli from July 2014.

© 2015, IJARCSMS All Rights Reserved