Computer Network & Communication

Shri Mata Vaishno Devi University Katra (J&K)

Project Report On

Seurity Issues In Cloud Computing

Under the Guidance of:

Deo Prakash

(Assistant Professor, SMVDU)

Submitted By:

Dharmveer Sharma

14BCS017

COMPUTER SCIENCE & ENGINEERING

Index:

(I) ABSTARCT :

Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so 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, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. This paper firstly lists the parameters that affect the security of the cloud then it explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It also discuses some tips for tackling these issues and problems.

General Terms

Cloud Computing, Cloud Security

Keywords

Cloud issues, Virtual machine layer, Data issues, Security issues

1. 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. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet . Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels . 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 .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. The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud. 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. This paper firstly lists the parameters that affect the security of the cloud in section 2. Section 3 explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues. Section 4 discuses some of tips and tricks to tackle these issues.

2. Parameters affecting cloud security

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.

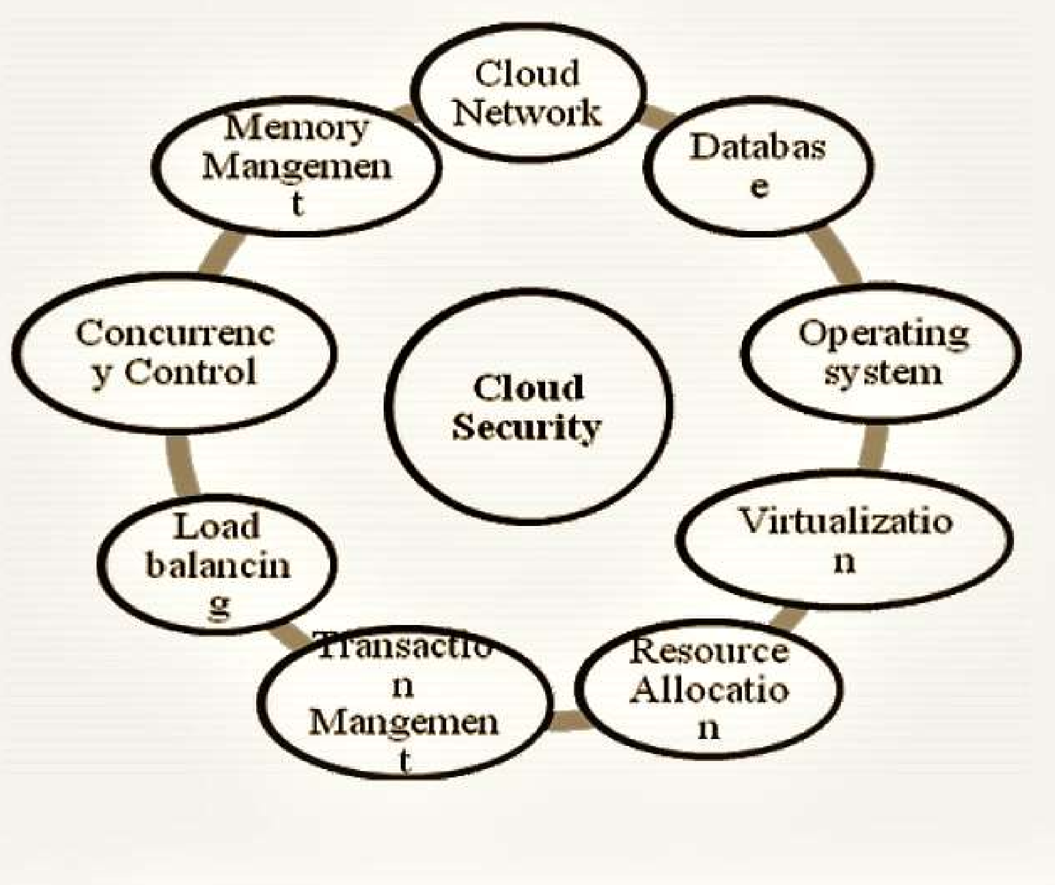


Figure 1: Parameter that affects cloud securit

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 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.

3. Security Issues faced by Cloud computing

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 . 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

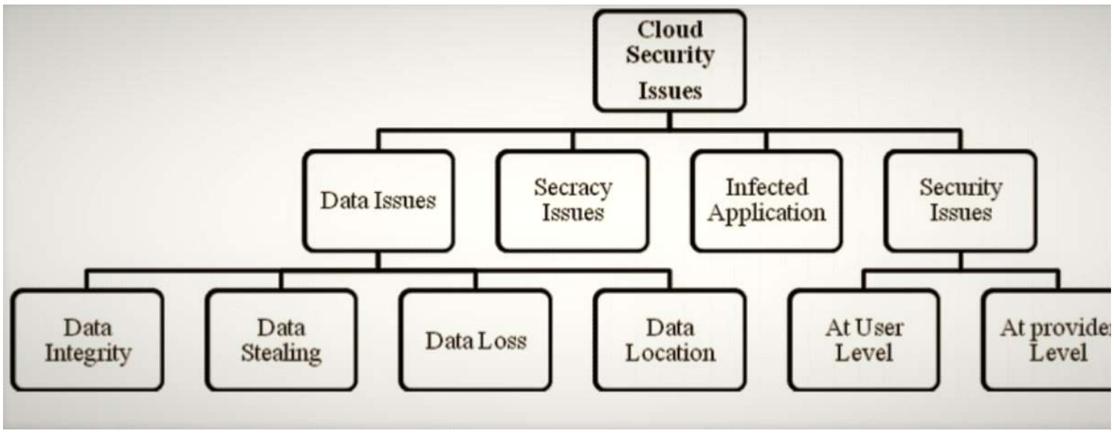


Figure 2: Cloud Security Issues

3.1 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 consumerand 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 accessesable 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.

3.2 Secrecy 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.

3.3 Infected Application:

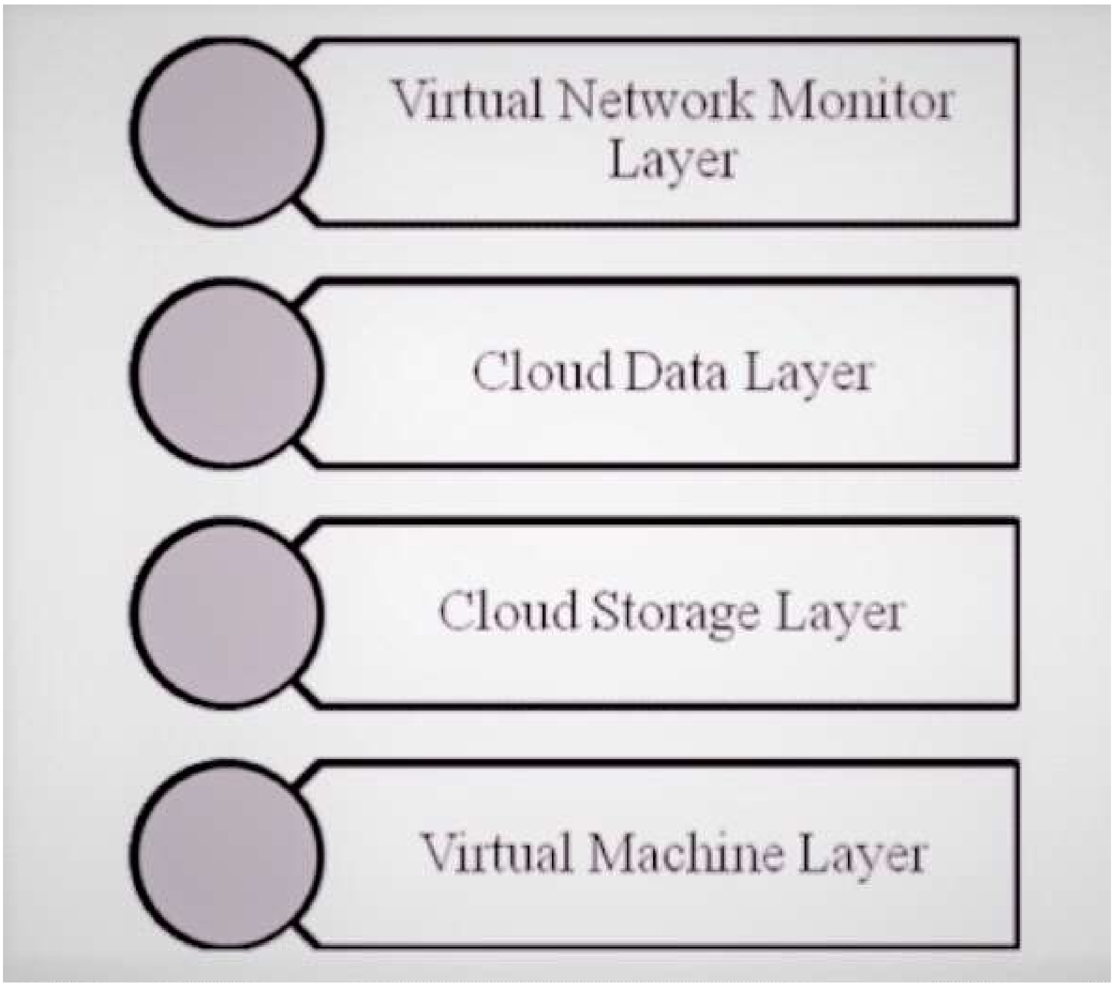
Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud whichwill severely affect the customer and cloud computing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

3.4 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.

4. Solutions and tips to cloud security Issues

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing environment. It consists of four layers as shown in



Virtual Network Monitor Layer

Cloud Data Layer

Cloud Storage Layer

Virtual Machine Layer

Figure 3: Layered Framework for Cloud Security

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN . However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers. There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

4.1 Verify the access controls:

Set up 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.

4.2 Control the consumer access devices:

Be sure the consumer's access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

4.3 Monitor the Data Access:

cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc.

4.4 Share demanded records and Verify the data deletion:

If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract .

4.5 Security check events:

Ensure that the cloud service provider gives enough details about fulfillment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider.

5. CONCLUSION

Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest gaps between cloudsecurity practice and cloud-security research theory lies in the fact that the assumptions in the research leave out some very important differences between actual cloud security and virtual machine security. Research should be center on these gaps and differences and its removal One of the pieces of the framework might be developing a way to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. People's behavior can be tracked and monitored for instance whether people allow the automated patching software to run, or updating anti-virus software definitions, or whether people understand how to harden their virtual machines in the cloud.

6.References

[1] http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud-Benefitsand-drawbacks.

[2] Michael glas and paul Andres, "An Oracle white paper in enterprise architectureachieving the cloud computing vision", CA-U.S.A, Oct 2010.

[3] 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.

[4] 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.

[5] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST, Germany.

[6] 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.

[7] Problems Faced by Cloud Computing, Lord CrusAd3r,

dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[8] 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