RESEARCH ARTICLE OPEN ACCESS

Solutions of Cloud Computing Security Issues

Jahangeer Qadiree [1], Mohd Ilyas Maqbool [2]
Research Scholar [1]
Aisect University
Institute of Science and Technology
India

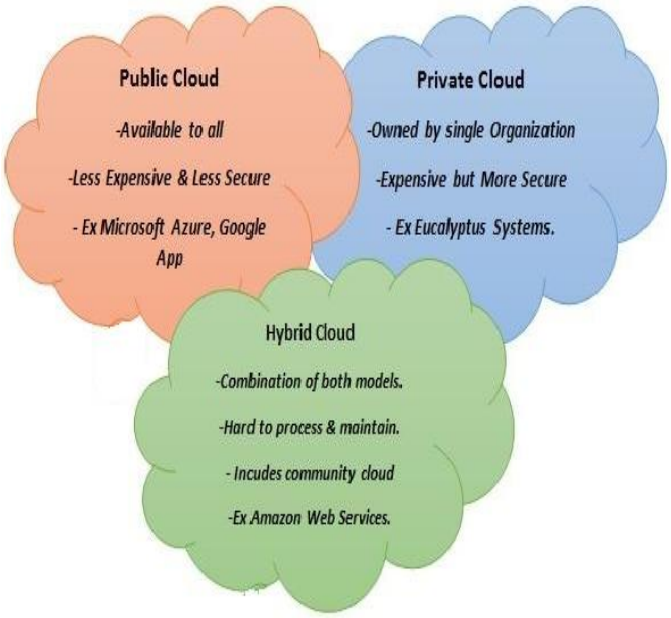
ABSTRACT
Cloud computing is a model which uses the mixture concept of "software-as-a-service" and "utility computing", and provides various on-demand services in a convenient way requested end users. It is internet based where resources are shared and the information is available for on demand service users. Security issue in Cloud computing is the important and critical issues because the resources are distributed. Both the Cloud provider and the cloud consumer should be fully sure that the cloud is safe enough from all the external threats so that the customer does not face any kind of problem like loss or theft of their valuable data. There is also a possibility where a malicious user can penetrate the cloud by imitate an authorized user, and affect with a virus to the entire cloud and affects many customers who are sharing the infected cloud. In this paper we firstly lists the parameters that affects the security of the cloud then it explores the security issues of cloud computing and the troubles faced by providers and consumers about their data, privacy, and infected application and security issues. It also presents some security solutions for tackling these issues and problems.
Keywords:- Cloud Computing, Data issues, Security issues.

I. INTRODUCTION

Cloud Computing is a computer based model that produce various services in the form of on-demand services, it is accessible worldwide to everyone, everywhere and every time, including clouds referring to the internet and the web. [1] [2]. In simple, Cloud Computing is the mixture of a technology that provides the hosting as well as storage service on the Internet [3]. Its main intention is to provide scalable and affordable on-demand computing structure with superior quality of service levels [4] [5]. Various international and national companies are developing and are offering cloud computing services but they have not properly considered the implications of accessing, processing and storing the data in a distributed shared environment. Many cloud-based application developers are struggling to include security. In various other cases, the cloud developers simply cannot provide real security with the currently affordable technological capabilities [6]. Cloud computing concept is simple to understand as it allows us to share the resources on a larger scale distributed networks which requires less cost and is location independent. Resources on the cloud can be used by the consumers and deployed by the vendors such as snapdeal, google, ibm, salesforce, zoho, rackspace, flipkart. Cloud computing model allows to distribute the required on-demand services for various IT Industries. Benefits of Cloud computing are broad. The very most important one benefit is that the users don't need to buy the resource from a third party vendor; rather they use the resources and pays for it as a service thus cloud helps the users to save time and also money. The Cloud Computing model is not only used by international companies but today it's also used by Small and medium enterprises [7].

Cloud Computing architecture consists of multiple cloud components interacting with each other for various data they are holding, thus allowing the user to access to the required data on a faster rate. When we look cloud it is more concentrated to the front and the back end. Front end is the user side who is accessed the data, whereas the backend is the data storage device, server which makes the Cloud [7]. Cloud computing is categorized into three different categories as per their usage include, private cloud, public cloud and hybrid cloud. The private clouds are maintained by single organization and the public clouds are maintained and are shared on a larger scale. The Private clouds provide better security control and more flexibility than other cloud types.

Hybrid clouds are the combination of Private clouds and Public Clouds that are used by various industries.



The benefits of cloud computing may be very appealing but nothing is perfect. Because the Cloud computing got many security issues especially on Data theft, Data loss and Privacy [7]. This research paper lists the parameters that affect the security of the cloud, explores the cloud security issues and problems that the cloud computing service provider and also the cloud service customer face by such as loss of data, privacy, infected application and security issues.

II. PARAMETERS AFFECTING CLOUD SECURITY

There are countless security issues for cloud computing as it surround many technologies include networks, operating systems, databases, resource allocation, transaction Processing, virtualization load balancing, and memory management and concurrency control [8].

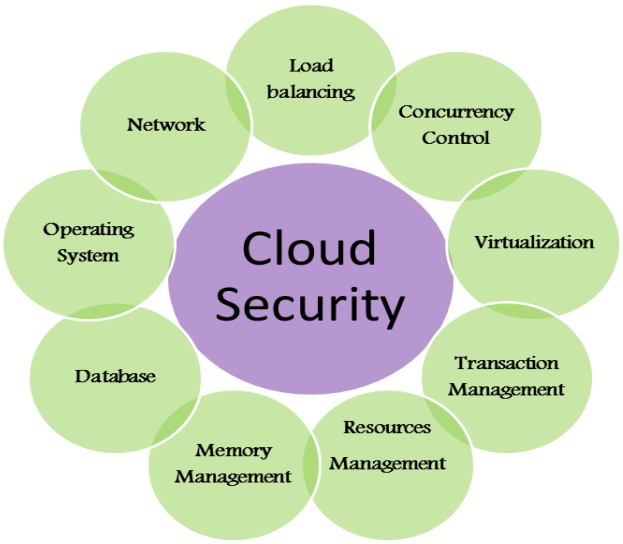


Figure 1: Parameter that affects cloud security

The various Security issues of these systems and technologies are appropriate to cloud computing systems. For example, the network that interconnects the systems in a cloud computing has to be secured. Moreover, the virtualization paradigm in the cloud computing results the various security concerns. For example, mapping the virtual systems to the physical systems has to be carried out securely. Data security includes encrypting the data as well as ensuring that the significant strategies are enforced for data sharing. Furthermore, the resource allocation and memory management algorithms have to be secured. Finally, data mining method may be applicable to malware detection in cloud computing.

III. VARIOUS SECURITY ISSUES FACED BY CLOUD COMPUTING

Whenever a discussion about security of cloud computing is taken place there will be a very much to do for it. The cloud computing service providers should be sure that their customers should not face any kind of problem namely loss of their important data or data theft. At cloud computing there may be a possibility where an unauthorized user can infiltrate the cloud computing by impersonating a legitimate user, there by infect the entire cloud with a virus. This leads to affect many customers who are sharing the infected cloud [7]. While discussing the security of a cloud, four issues are raised.

a. Data Issues
b. Privacy issues
c. Infected Application
d. Security issues

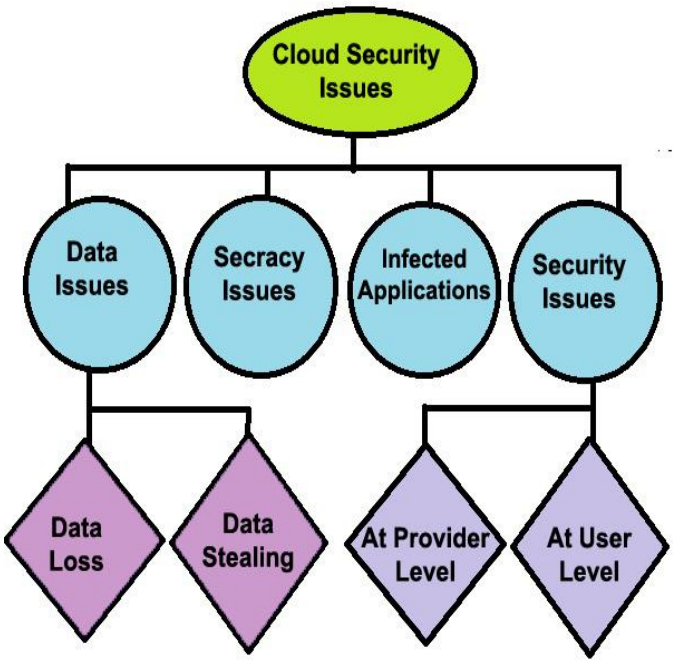


Figure 2: Security Issues of Cloud Computing

A. Data Issues:

In a cloud computing environment sensitive data arise as a serious issue regarding to security in cloud computing based systems. Firstly, when the data is on cloud, anyone can access data from anywhere and anytime from the cloud because the data may be usual, private and sensitive data in a cloud. At the same time, many cloud computing service customers and providers are accessing and modifying the data. So there is an important requirement for data integrity method in cloud computing environment. Secondly, the data embezzlement is another big serious issue in cloud computing environment. As we can say that many cloud computing service providers do not have their own servers, they buy the servers from other service providers due to it is cost effective. So there is a probability that data can be stolen from the external servers. Thirdly, Data loss is a very common problem in cloud computing environment. Whenever cloud computing service providers close their services due to some financial or legal issues then there will be a loss of data for the customers. Moreover, data can be damaged or corrupted due to some miss happening, natural disaster, and fire. Due to above condition, data may not be accesses able to the cloud computing service providers customers. Fourthly, data location is also an important and common security issue that requires focus in the cloud computing environment. Because the physical location of data storage is very important and crucial in the cloud computing. Data should be in transparent manner to from the users view.

B. Secrecy Issues:

The service providers of cloud computing should kept in mind that the customers important information is fully secured from other service providers, customer and user. As the most of the cloud servers are external, the cloud service provider should make it clear about who is accessing the data and also keep it well clear that who is maintaining the server so that it will help to the provider to secure the customer's personal data.

C. Infected Application:

The cloud computing service providers should have the complete control and access to their servers, so that they can monitor and maintain their servers. This will cause the hindrance to the malicious user from uploading any virus affected application onto the server which will seriously affect the user and cloud computing service.

D. Security issues:

The security of cloud computing must be done on two sides. Cloud computing service provider's side and the customer's side. The Cloud computing service developers should be fully sure that their server is secured from all the outside environmental threats that may arise in the cloud. They should also provide a good security layer to their customers; before using the services of cloud computing the user should also make sure that there should not be any kind of data loss or theft or tampering of data for other customers who are in the same cloud. A cloud is good only when there is a good security mechanism provided by the service provider to its consumers.

IV. CLOUD COMPUTING SECURITY ISSUES SOLUTIONS

There is a dire need for extended and advanced technologies, concepts and methods which leads to secure cloud. There is a layered framework available that assist security in cloud computing environment. The framework consists of four layers. [8].

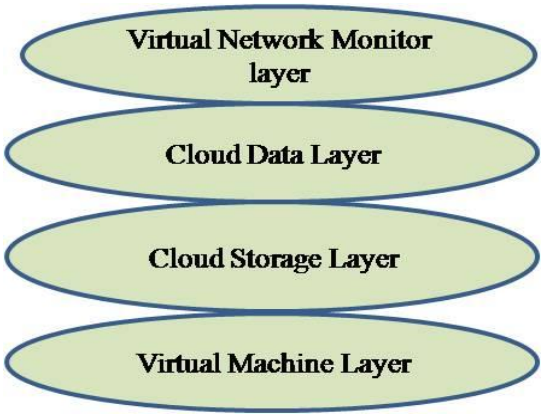


Figure 3: Cloud Security Layered Framework

First layer is secure virtual machine layer. Cloud storage layer is the second layer of cloud computing. It has a storage structure that integrates various resources from various external cloud service providers, so that it can build a heavy virtual storage system. Virtual network monitor layer is the fourth layer that combines both of the hardware and software mixture in the virtual systems to handle the problems [8]. However, there are various groups who are working and interested in developing standards and security strategies for clouds. The Cloud Security Alliance provider should describe the strategies and should also be ensured that the cloud can be used or accessed only by the authorized users.

CONTROL THE ACCESS DEVICES OF CUSTOMERS:

The cloud service providers should be sure about that the customer's access devices include Desktop Computers, virtual terminals, gazettes, and even a simple mobile phone are fully secured. Any kind of loss or theft to the customer's access devices or any unauthorized access to their devices by any unauthorized user can affect the whole security protocols in the cloud computing environment. The cloud service providers should adopt the desired policies, methods so that the user computing devices are maintained properly and are fully secured from any kind of malware detection and lead to assist the advanced identity features.

MONITOR THE DATA ACCESS:

The cloud service providers should be fully assure about that who is accessing, when and what kind of data is being accessed for what purpose. Because many servers had a common security complaint for their customers regarding snooping activities by many users's about their personal data.

SHARE DEMANDED RECORDS AND VERIFY THE DATA DELETION:

If any time the user or consumer needs to report its action, then the cloud service providers will share the diagrams or any other necessary information or we can say that the service provider should provide the audit records to the consumer or user. The cloud computing providers should also verify the proper deletion of data from shared or reused devices. As Many Cloud providers do not provide the proper remover of data from the drives each time thus in result the drive space is forsaken. [6].

SECURITY CHECK EVENTS:

It should also be ensured that the cloud service provider gives sufficient details about fulfillment of assurance, break remediation and reporting contingency. These security check events will describe the responsibilities, declarations and the required tasks of the service providers.

V. CONCLUSION

The cloud computing service provider and the consumer should be fully sure about that their cloud is fully protected from all the external threats or attacks, so there will be a strong and mutual interpretation by both of the customer provider. The largest gaps between cloud security applications and research theory lies in the fact that the assumption in the research leaves some important differences among the actual cloud security and the virtual machine security. Research should be center on these gaps and differences and its removal. One of the pieces of the framework might be for developing a strategy to monitor the cloud computing software, and theanother might be the development of the isolated processing for the applications of specific clients'. The consumer's behaviour can be traced and monitored for instance whether the consumer allows the automated patching software to run, or updating the anti –virus definitions, or whether the people understand that how to solidify their virtual machines in the cloud.

REFERENCES

[1] Michael glas and paul Andres, "An Oracle white paper in enterprise architecture achieving 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-issueswithcloud-computing-in-10-steps.

[6] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf

[7] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(S. Kuppuswamy, P. B. Shankar Narayan, "The Impact of Social Networking Websites on the Education of Youth", In International Journal of Virtual Communities and Social Networking, Vol. 2, Issue 1, page 67-79, January-March 2010.

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

AUTHOR PROFILE

JAHANGEER QADIREE is presently pursuing his **Doctor's Degree (PHD)** in Information Technology at Aisect University, Institute of Science and Technology. He has received his Bachelors Degree in 2011 from Computer Application with 75% and Masters Degree in the discipline of Information Technology with 84.5% in the year 2014 from Aisect University. His research area is Networking, Software Engineering. Cloud Computing, Data Mining.

MOHD ILYAS MAQBOOL has received his Masters Degree in 2011 in the discipline of Information Technology from HNB Gharwal University Uttrakhand and M.Phill Degree in Information technology from Bhagwat University Ajmer. His research area is Cloud Computing, Software Engineering, and Data Mining.