RESEARCH ARTICLE OPEN ACCESS

Security Threat Issues and Countermeasures in Cloud Computing

Jahangeer Qadiree [1], Trisha Arya [2]
Ph.D. Scholar [1]
Department Of Information Technology
Aisect University, Institute of Science and Technology, Raisen
MP- India

ABSTRACT
Cloud computing field has reached to the highest level of technical heights. The security problems of cloud computing hinders its development. It is totally internet based technology where the resources and information shared on a distributed network. So it is important for both provider as well as consumer to provide the security and trust to share the data for developing cloud computing applications. Because now organizations are now moving fast towards the cloud. So there is the possibility of threats that will harm the data on the cloud. In our paper we mainly focuses on security threats of cloud computing system also we mention some solutions and countermeasures on these security problems

Keywords:- Cloud Computing, Threats, Security issues, Countermeasures.

I. INTRODUCTION

Cloud computing is the fastest growing industry. It is the advanced and emerging technology in which the data is distributed over a virtual network and the resources are shared at a very low cost. [1]. Cloud computing concept is simple to understand, as it is the mixture of technology that provides hosting and storage service on the Internet [2]. The main goal of the cloud computing environment is to provide the scalable and inexpensive on-demand computing infrastructure with a very good quality of service levels [3] [4]. Various international and national level companies are developing and offering the cloud computing environment products and services but unfortunately they have not properly considered the implications of storing, processing and accessing data in a distributed environment. In fact, many cloud developers of cloud-based environment applications are in struggle to include the security mechanism. We can say, that the cloud developers or providers simply are not providing the real security with the currently affordable technological capabilities [5]. In the cloud computing environment the resources are shared on a larger scale which is cost effective and location independent. The resources on the cloud computing environment can be used by the consumers that are deployed by the vendors like amazon, GOOGLE, IBM, SALESFORCE, ZOHO, RACKSPACE, and MICROSOFT. It also allows to share the necessary software's and the required tools for various IT enabled Industries. Cloud computing environment benefits are enormous like that the cloud computing consumers are totally free to buy the resource that they are needed them from a third party vendor, either they can use the resource and will pay for it as a service thus helping their customer to save both time and money. Cloud computing environment is not only for the Multinational companies but Small and medium type enterprises are also using the cloud computing environment [6].

II. CLOUD COMPUTING BLOCKS

The architecture of the Cloud computing environment consists of various cloud components interacting with each other for the data they are holding on, thus permit its users to access the required data on a faster rate.

The cloud computing environment is divided into two categories: the front end and the back end. Both of the sides are connected to each other via internet. While discussing the front end side it is the user's side who are using the cloud services provided by the back end side which is the cloud providers side [7].

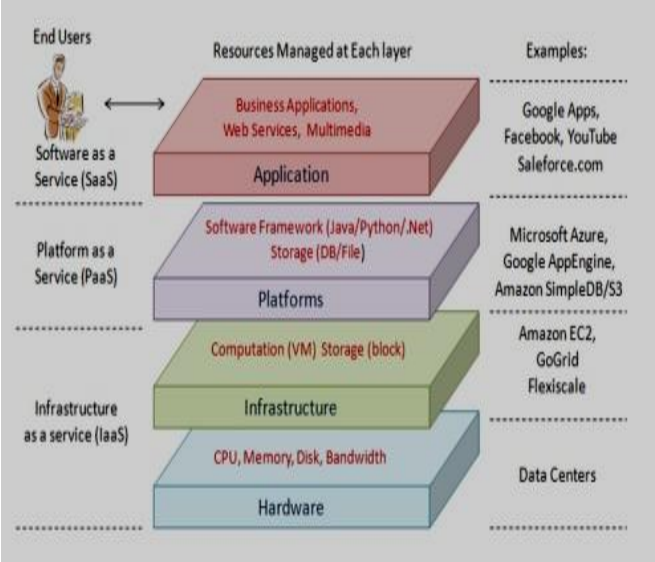

Fig 1: High Level View of Cloud Computing Architecture

The cloud deployed model services can be categorized into three types first one is Software as a Service (SaaS), second one is the Platform as a Service (PaaS), and the third one is Infrastructure as a Service (IaaS).

- ***Software-as-a-Service (SaaS)***: SaaS can be defined as the delivery method of software that allows the cloud users to use the software and its benefits remotely as a web based service. The consumers use the SaaS and pay for its services as monthly basis. Because the software's are hosted and maintained by the application service providers. [7].
- ***Platform as a Service (PaaS)***: PaaS is the cloud service that allows the developers to develop software applications by using the provider's tools. It consists of preconfigured features. PaaS is paid on the subscription basis. The infrastructure is managed for the customers. The developers need to pay it only for the subscription basis, not to invest in physical infrastructure. Force.com, Google App Engine and Microsoft Azure are the examples of PaaS:.
- ***Infrastructure as a Service (IaaS)***: this type of service can be defined as the sharing of hardware resources for executing the services using Virtualization technology. IaaS makes the resources accessible such as servers, network and storage by applications and operating systems. It gives the access to the clients to to build their own information technology platforms. Its services can be accessed at any location because it is a location independent. The clients plays only the resources that they are using. Its resources are available all time.

The environment of cloud computing is divided into three different categories as per their usage and requirement include, private cloud, public cloud and hybrid cloud.

- ***Private cloud***: Private clouds are owned by the single organization. The private clouds provides better control and more flexibility. They are very expensive and secure when we compare them to other clouds. The providers and the users have a very good control of the cloud infrastructure. One of the best examples of a private cloud is Eucalyptus Systems [8].
- ***Public Cloud***: These Type of cloud are totally hosted and maintained and are shared on a larger scale. Consumers pay for the resources that they use. Users have a little control over the cloud infrastructure. Microsoft Azure, Google App Engine are the examples of public clouds.
- ***Hybrid Cloud***: Hybrid clouds is the composition of two or more cloud models, linked each other in a way so that the data transfer takes place between them without affecting each other. These types of clouds are created by the large enterprise. In this model, the company outlines the main goals and requirements of services [9]. But the major drawback of the hybrid cloud is the difficulty in effectively creating and governing such a solution.

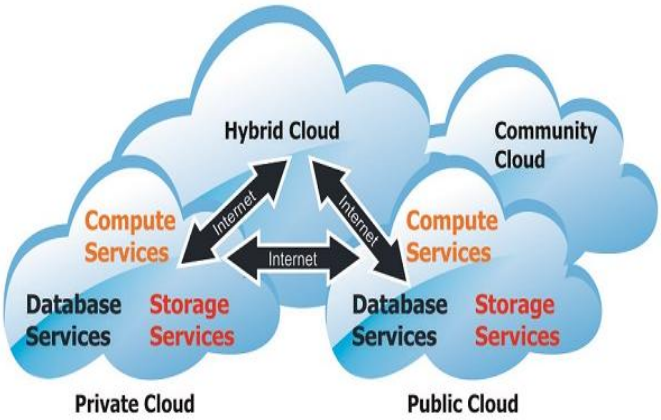

Fig 2: Deployment Models of Cloud Computing

III. CLOUD COMPUTING SECURITY ISSUES

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].

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 of virtual systems to the physical systems should be carried out securely. Data security includes encrypting the data as well as ensuring that the significant methods are enforced for data sharing. Furthermore, the resource allocation and memory management algorithms should be secured. Finally, the data mining strategy will be applied for malware detection in the cloud computing environment. While discussing the security issues there raises four types issues in cloud.

- Data Issues
- Privacy issues
- Infected Application
- Security issues

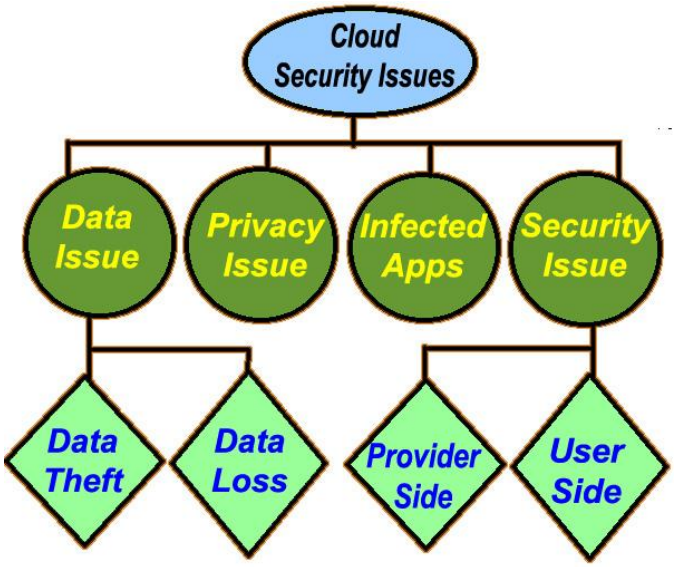

Fig 3: Security Issues of Cloud Computing

- ***Data Issues:*** In the cloud computing environment sensitive data emerges as a big issue with regard to the security in the cloud based systems. Firstly, when the data is on the cloud, consumers from anywhere and anytime can ingress the data from the cloud environment so the data may be common in the cloud. At the same time, various cloud computing service customers and also the provider can access and modify the data. So there is a dire need of some data integrity mechanism in the cloud computing. Secondly, data stealing is one of the enormous and serious issue in the cloud computing environment. There are many cloud service provider who don't have their own servers instead they buy the servers from other organisations. So there is a chance that the data can be stolen from the external server. Data loss is the common problem faced in the cloud computing. Sometimes the cloud computing providers closes their services due some financial or legal issues; at that time their customers will lose their valuable or important data. Moreover, the data can be lasted or corrupted due to some technical faults or fire. Due to the above conditions, the user can not access the data and suffers very badly. Location of data is another enormous big issue that requires a serious focus in the cloud computing environment. The physical location of the storage is very important and critical. It should be clear to the users. The Vendors should not reveal where all the data's are stored.
- ***Privacy Issues:*** The cloud computing service providers should make sure that the customer's information is well secured from all the threats. As most of the servers are external, the providers of cloud services should make sure who is accessing the data and who is maintaining the server so that it enables the provider to protect the customer's personal information.
- ***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. This will benefit the provider to prevent the unauthorized or malicious user to access the cloud and restrict him from uploading any kind of virus infected material to the server that causes cloud computing service badly.
- ***Security issues:*** The security mechanism of the cloud computing environment should be done on two sides namely cloud providers side as well as consumer's side. The providers of the cloud computing should be fully sure that their server is well secured from all of the attacks that may come across. The provider has to provide a good security layer to their users, so that there should not be any kind of data theft of loss.

.

IV. CLOUD COMPUTING SECURITY THREAT COUNTERMEASURES

There is a dire need to extend the latest available technologies and security methods, so that the cloud computing model will be fully secure. In the cloud computing model there is a layered framework available that will assist a good security in the cloud computing. The layered framework consists of four layers.

There are various communities who are working to develop the useful security mechanisms for cloud so that the cloud will be accessed only by the authorized users.

- **Control the Customers Access Devices:** The cloud owners should protect the consumer's access devices includes computers and mobile phones etc., from all the threats. The providers should adopt the best mechanism so that unauthorized user or malicious user can not access the consumer's access devices and the consumer's data will be fully secured from any kind of attacks.
- **Data Access Monitor:** The data access monitoring should be fully maintained by the providers, so that the complaints of users regarding snooping their data should not be taken. Because snooping of data is the common security complaint of the servers.
- **Data Deletion Verification:** As many of the cloud providers do not remove the data from the drives each time from their side when the user deletes their data. Thus leads the storage errors. The providers should provide the necessary information that their consumers need. So that the drive space should not be forsaken.
- **Security Check Points:** The cloud providers should adopt the necessary security check points on their server. So that it will help to describe the responsibilities and another sufficient activities from both service providers as well as service users.

V. CONCLUSION

The sharing of resources in a distributed environment is one of the most panic in providing security in cloud computing platform. The cloud computing service provider's should inform to their consumers regarding their security policies used on their cloud. In our paper, firstly we discuss the blocks that are present in cloud architecture. We also highlight the deployment model and then we focus the various security issues and research challenges in the cloud computing environment and also the available countermeasures that deals with the security thefts. Security of data is the major issue for Cloud Computing. There are several other security challenges namely the security aspects of network and the virtualization. In our paper we highlighted all these issues of cloud computing. We trust that due to the complexity of the cloud environment, it becomes arduous to fulfil the 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.

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-issues with cloud -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.

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

[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

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, and Complier Design.

TRISHA ARYA has received her Bachelor's Degree in 2011 from Computer Application with 71 % and Master's Degree in the discipline of Computer Application with 75.42 % in the year 2012 from RGPV University. She Has Worked at Aisect University as a Head of Department in the Dept. of Computer Science And Application, her research area is Networking, Software Engineering. Cloud Computing, and Data Mining.