CLOUD COMPUTING: THE TECHNOLOGY & ITS SECURITY CHALLENGES

[1]SIDDHARTH PANDA, [2]TANZEEM RAHAMAN

Wipro Technologies, Hinjewadi, Pune
E-mail : [1]siddharth.panda16@gmail.com, [2]tanzeem133@gmail.com

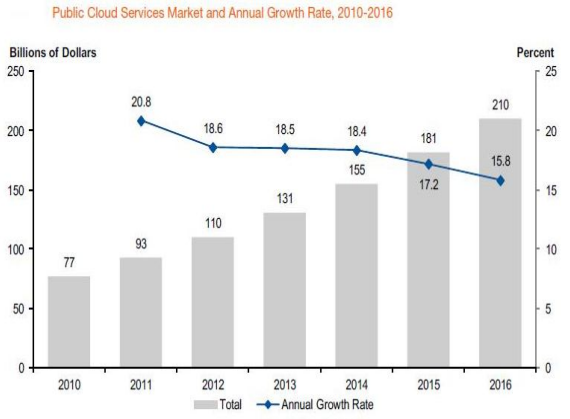
Abstract— Cloud is a platform for storing large amount of data. Cloud computing offers businesses and organizations an opportunity to leverage information technology without significant initial investment. Implementation of cloud computing services minimizes local storage trust in addition to decreasing operational and maintenance costs. As good a boon it appears to be, the adoption of cloud computing is impacted by a questionable security model. Security is one of the major issues which reduces the growth of cloud computing due to feeble data privacy and data protection. In this paper, the extreme focus is given to the security challenges related with cloud's service models, deployment models, and issues related to networking capabilities are discussed and studied.

Index Terms— Cloud computing, IaaS, PaaS, SaaS, types of clouds, cloud security challenges.

I. INTRODUCTION

Cloud computing is a model that enables the development, deployment and delivery of products and services to the customers with a pay-as-you-go model. It is a service model that involves the idea of storing and accessing the resources over the Internet rather than storing them onpremise. Basically, cloud computing has motivated academia, industry, businesses to take over this technology to host their applications on the cloud so as to cut-off the cost of buying the on premise local server. As per Gartner survey, the cloud market was anticipated to rise from $76.9B in 2010 to $210B in 2016.These revenues connote that it is a promising platform.Cloud computing is a model which provides on-demand delivery of Information Technology (IT) related capabilities or resources through the Internet to the outside world.In cloud computing systems, the data is stored on remote servers& accessed through the internet.

Nowadays, cloud computing is a growing area that involves wide range of new technologies and applications that touches almost every house residents. Among the associated concepts with this area is the Mobile Cloud Computing (MCC) which basically allows the users to access and use the cloud services and applications via mobile devices.Cloud storage services are used widely to store and automatically back up arbitrary data in ways that are considered cost saving, easy to use and accessible. They also facilitate data sharing between users and synchronization of multiple devices.But and as we know, the mobile devices have number of challenges that limit their performance, such as battery life time, and lack of computing resources and storage. Another important issue in Cloud and Mobile Cloud Computing is the security of the stored data. There are vital data that is processed and stored in the cloud systems. Losing or exposing these valuable data will have a terrible impact on the data owners being individuals or organizations. And so, there is an increasing demand to protect data over the cloud systems.In this paper, we have discussed cloud computing technology and extreme focus is given to the security challenges. This paper tries to give you a basic understanding of cloud computing and explores the cloud computing aspects and then puts forward the issues related to its security.



II. CLOUD COMPUTING: THE TECHNOLOGY

A. HISTORY:

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. The concepts behind cloud computing dates back to 1950s. At that time, large-scale mainframe computers became available in academia and corporations. These were accessed via thin clients/terminal computers, often referred to as "dumb terminals", called so because they were used for communications but had no internal processing capacities. To make a better use of costly mainframes, a practice was developed that allowed multiple users to share both

the physical access to the computer from multiple terminals as well as to share the CPU time. This eliminated periods of inactivity on the mainframe and allowed for a greater return on the investment. The sharing of CPU time on a mainframe was known in industry as time-sharing. The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to a growth in cloud computing.

B. SERVICE MODELS:

Software as a service (SaaS): SaaS is a software delivery model that provides access to software and its functions operating on a remote cloud infrastructure offered by cloud providers. Salesforce.com offering in the customer relationship management (CRM) space was the innovator to provide software as a service. Other examples include online word processing and spreadsheet tools, Gmail, WhatsApp, and SAP.

Platform as a service (PaaS): PaaS provides the framework for deploying and delivering of applications and services. It allows developers to develop new applications without any pressure of buying expensive tools and managing the local servers. Examples include Hadoop, Microsoft Azure, Force.com, and Google App engine.

Infrastructure as service (IaaS): IaaS provides the infrastructure such as network, memory, storage, processor to the users on demand. Examples include Amazon EC2, Windows Live Skydrive, and Rackspace Cloud.

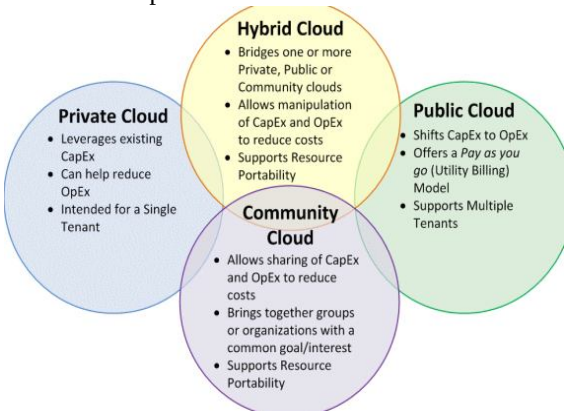
C. DEPLOYMENT MODELS:

Private cloud: Suppose that a business is connected with highly sensitive data related to financial and security transactions. Naturally data should beprotected from competitors and hackers. At the same time the business also wishes to use the cloud services. This is where private cloud comes into service. It gives complete security systems fortified with firewalls, leased lines, on site hosting, inline configured network, dedicated resources, fail proof systems etc.

Public Cloud: Public cloud does not mean that anyone can access anyone'sdata. It just means the resources are shared with other users in the services space. Security systems are installed in this model also. Data and resources of one client will never be accessible to others unless the OWNER grants access permissions. This model can host generic and shared data, software applications, Database systems, platforms and infrastructural elements. For example, one can host online conferences with overseas clients, vendors and in-house technical team through the public cloud.

Hybrid Cloud : This is essentially combination of private and public clouds. One can keep critical data, resources and applications in the private part and the non-critical elements on the public part. This gives the organization or individual a freedom to shift any of the services from one cloud to the other.

Community Cloud : A cloud environment accessible only by organizations with similar interests.The community cloud is used where several organizations share the similar infrastructures. It may exist on premise or off premise.



III. CHALLENGES IN CLOUD COMPUTING

Now the question arises, if cloud computing is so powerful, why isn't everyone adopting it?

- In the cloud, the clients don't have knowledge about what's happening inside.
- In addition to this, even if the cloud provider is honest, it can have eavesdropper who can fiddle with the VMs and defiles confidentiality and integrity.
- Clouds are still susceptible to data confidentiality, integrity, availability,

privacy issues plus some internal and external attacks.

There are several challenges in cloud computing which are necessary to keep in knowledge and be aware about these. Some of the challenges are given as follows

Privileged User Access: If any sensitive data of client is accessing outside the enterprise then client needs to buy a new membership for verification otherwise the risk of data leak is increased.

Availability: Some clients of cloud computing need to access the cloud services but the range of the company is not available at every time and place.

Regulatory Compliance: Cloud computing provider never allows any external audits and also refuses to install new security certificates to network.

Data Location: When a client uses the cloud computing then client doesn't know about the location where his data is stored. And hosted from where?

Investigative Support: If any inappropriate and illegal activity takes place with client data in cloud computing then the proper investigation about this is impossible.

Data segregation: In cloud computing, the data of client is available in a shared condition with other clients of cloud that is using services in parallel.

Recovery: If server or data center ruined due to some natural problem or disaster, the cloud provider informs the client about the status of his data.

IV. SECURITY RISK IN CLOUD COMPUTING

Cloud computing is a way of accessing resources and service for a particular organization. But hacker, attacker and security researcher find out that cloud computing is not fully secure. It has some issues which are mentioned below

Insecure Interface: Cloud service provider show all the software interface and application which are used to interact with cloud by client. Data arrangement, identity management, monitor of service all happen on the cloud. And authentication and access control is monitored by these interfaces too

Data Loss or Leakage: When cloud computing is being executed. There are two changes happen to the client data. Firstly, data is stored far from the client machine. Second, data is transmitted from one execution mode to multi execution mode. When these changes occur to information place the security issue of data loss or leakage.

Malicious Insiders: At this time, cloud is served by organization which hires employees for providing service to its client. So those employee can misused the information or can sell information to other organization and this is happen on internal level of a company and hard to aware for clients or consumers.

Shared Technology: components of working under the cloud which make environment (virtual memory, processor, caches etc) for computing does not support strong isolation for multi execution mode

Flood Attacks: When any customer is using the cloud computing services and he need to extend size of service and initialization is happen due to dependency on internal communication. And attacker makes large false request to the server. So server gets busy and unable to work properly.

IP Spoofing: IP spoofing is known as analysis of network traffic. When any attacker send message to a computer being a trusted user. Attacker determines the IP address of a trusted system and makes some modification to packet information like packet header and sends that packet which seems as packet is originating from trusted system.

DDOS Attacks: In DDOS (Distributed Denial of Service) attack, attacker makes some spoofing and sends large number of requests to the server. So server gets busy and not able to response on the valid and authentic request of customer. In this way server deny for giving the service to customer and DDOS take place

V. PRIVACY ISSUES IN CLOUD COMPUTING

Client uses all services which are server oriented and all processes have to be complete on the server. Due to server computing, all the data of client is saved at server which can be called as data center. But some issues may be arises in the regard of privacy. Some privacy issues are explained in this paper as

Loss of Control: When a client is using cloud it means he is using some applications in cloud and makes some document and project under those applications which stored on cloud. If client needs to change cloud provider then he can be threaten about manipulation or misuse of his sensitive information which he already store on the present cloud data centers.

Invalid Storage: The data may be stored on an inappropriate space or secondary memory of the cloud because if authentic storage is used then cloud provider has to pay for use of storage which reduces the profit of cloud provider. So this may be a serious issue about data privacy in cloud computing.

Access Control: When client saves his complete data to the server and he is not accessing it for a long time due to any reason. An unauthorized access will use that data illegally due to lack of authorized rights of access control.

Data Boundary: Cloud provider makes several copies of data to provide at the location for client. Wherever this data is required by a user, it is available there for use. If any data present at the data center is not used for a long time then it deleted from data center. And multiple copies of data for servers can be cause of information leak or theft.

CONCLUSION

Today, cloud computing is the technology being talked across industries due to its efficiency, the flexibility of resources, pay-per-use model, dynamic scalability, faster time-to-market, increased collaboration and cost efficiency. Despite its advantages, many organizations are still not adopting it because of security reasons associated with it. The cloud computing has potential to deal with future needs and it will be a milestone of future computation architectures. But we need to work on its data security & data privacy to improve its performance index and to make it a more suitable candidate for future needs.

Cloud is a revolutionary technology and with its proper development, it can change the face of almost all computational models.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing

[2] AkhilBehl, KanikaBehl "An Analysis of Cloud Computing Security Issues" 2012 IEEE

[3] Anas BOUAYAD, Asmae BLILAT, Nour el houda MEJHED, Mohammed EL GHAZ "Cloud computing : security challenges" 2012 IEEE

[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom "Cloud Computing Security: From Single to Multi-Clouds" 2012 45th Hawaii International Conference on System Sciences

[5] Wei Zhao, Yong Peng, Feng Xie, Zhonghua Dai "Modeling and Simulation of Cloud Computing: A Review" 2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC)

[6] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari. 'A secure cloud computing model based on data classification.' Elsevier, pp 1153-1158, 2015.

[7] N. Sengupta and R. Chinnasamy. 'Contriving hybrid DESCAST algorithm for cloud security.' Elsevier, pp 47-56, 2015.

[8] S.K. Sood. 'Hybrid data security model for cloud.' International Journal of Cloud Applications and Computing, pp 50-59, 2013.

[9] Satveer Kaur and Amanpreet Singh, "The Concept of Cloud Computing and Issues Regarding its Privacy and Security", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 3, May 2012.

[10] FarzadSabahi, "Cloud Computing Security Threats and Responses", 2011 IEEE 3rd International Conference on Communication Software and Network (ICCSN), pp. 245-249, May 2011.

★★★