Cloud Computing: Security Issues

Nivedita M. Mathkunti

***Abstract*—Cloud computing is a present and future of the Technology (IT), to enhance the capacity of Information dynamically without investing capital for new infrastructure, training new personnel or licensing new software. With extending the IT's present capabilities, it is growing radically. Enterprise customers are unenthusiastic to deploy their business in the cloud, because of security of the cloud computing. In this study, a survey of the different security risks is presented with proposal of new idea to build cloud with optical network which is suitable for the access network is considered as the one of highly secured for the cloud because of its optical devices.**

***Index Terms*—Cloud computing, cloud computing security, cloud computing issues.**

I. Introduction

Cloud computing is an evolving paradigm, according to National Institute of Standards and Technology (NIST), cloud computing is not having perfect definition. NIST defines cloud computing as a model for enabling convenient, on–demand network access to a shared pool of configurable computing resources like servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction, around us its definition, attribution and characteristics are still being debated by the public and private sectors. So we can accept it as "evolving paradigm" [1].

Cloud computing promotes the availability of data, for this objective, it is composed of five essential characteristics. Service models and deployment models [1] in cloud computing services and applications will migrate towards this paradigm.

Fig. 1 gives the whole picture of Cloud Module. The three main services of the cloud are shown in this module. The thin-clients [1] on user devices access, over the network applications hosted in data center by application service provider. In cloud computing the critical situation is that the services are delivered from locations that are the best for the current set of users.

This can also be achieved when the services will be hosted on Virtual Machine (VM) in interconnected data centers and these VMs also migrate towards the location which suits for current user populations [2].

Technically cloud computing can be defined as a Transport Control Protocol/Internet Protocol(TCP/IP) based high development and integrations of computer technologies such as fast microprocessor, huge memory high speed network and reliable system architecture. Today we are utilizing the cloud computing which is exist because of standard inter-connected protocols and matured assembling data center technologies [3]. Oracle CEO L Ellison said that, *"cloud computing is nothing more than everything that we currently do"* [4].

The other advanced technical definition of cloud computing as the development and adoption of rapidly evolving technology, strong fault tolerance, TCP/IP based and virtualized. These characteristics are partially supported by grid computing. High security is not yet ensured completely.

There are many more definitions for cloud computing these will focus on certain aspects of the technology. From these definitions any one can get confusion about what cloud computing really is what the services are provided by it and how it is deployed and so on. The answers to these questions are not certain. Cloud computing is also distinguishes itself from other computing paradigms like *grid computing*, *global computing*, *internet computing* in the various aspects like on-demand service provision with guaranteed Quality of Service [QoS], autonomous system, user centric interfaces, the other techniques that contributes to the cloud computing are *virtualization*, *Web Service and Service Oriented Architecture* (*SOA*), *Web 2.0* and *mash up Application Programming Interface* (*API*).

It also includes SOA and virtual applications of both hardware and software. The cloud environment also provides a scalable services delivery platform. It shows its resources at various level consumers vendors and partners. The main basic services delivered by cloud are Platform as a Service, Software as a Service, and Infrastructure as a Service. Infrastructure service allows getting use of hardware or infrastructure.SaaS allows getting the software middleware/ traditional customer relationship management as a service.

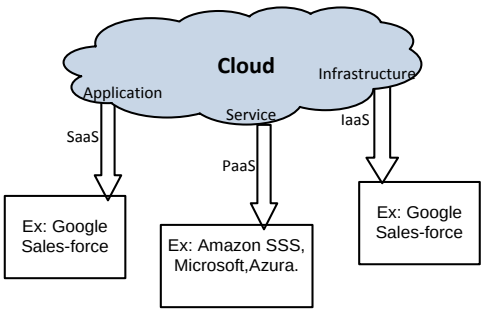

Fig. 1. Cloud module.

PaaS offers the software execution environment [5]-[7]. The PaaS application server enables the lone developers to develop web based applications without buying actual servers and setting them up. This model has to protect data, which is

Manuscript received February 11, 2014; revised April 2, 2014.

Nivedita M. Mathkunti is with the Alliance College of Engineering and Design, Alliance University, Bangalore-562106, Karnataka, India (e-mail: nivedita.manohar@alliance.edu.in).

[1]Thin Clients: Clients are a computer which does not have internal hard drive, but rather let the server does all the work, but then displays the information.

DOI: 10.7763/IJCCE.2014.V3.332

especially essential for storage. For congestion there is the problem of outage from this cloud environment so the high priority for security against outage is given. The cloud services can be deployed in four ways depending upon the customers' requirements as public cloud, private cloud, community cloud and hybrid cloud. The cloud services can be deployed in four ways depending upon the customers' requirements as public cloud, private cloud, community cloud and hybrid cloud.

Private cloud: A cloud infrastructure is made available only to specific customer and manage either by the organization itself or third party service provider. These are designed and managed by the information technology department of the organization for which this cloud is designed. Its objective is to provide services internally to an organization. It gives the high level of control over the cloud services and the infrastructure [8]. The private cloud model, which is defined as cloud computing on private networks or internal clouds, is having a best example of private cloud - Defense Information Systems Agency (DISA). It is a private cloud available at its in-house Defense Enterprise Computing Centers (DECC) on which it currently hosts Managed Service Providers software.

Public cloud: These infrastructural models are off premise and run by a third party. These are stand alone or proprietary [9]. The examples of these clouds are Google, Amazon, Microsoft and others. These public clouds usually deliver the request with mixing applications from different consumers on shared infrastructure [8].

Community Cloud: More than one organization shares this module and managed by them or service provider [5].

Hybrid cloud: A composition of two or more cloud deployed models linked in a way that data transfer takes place between them without affecting each other. Now-a- days, technological advancement made us to avail the derivative cloud by deploying various cloud models. Example Mobile Cloud Computing (MCC) which is the result of emergence of high end network access technologies like 2G, 3G, Wi-Fi, Wi-MAX etc. *Pre-cloud phase* is followed by the ideation phase during the 1999 to 2000s. During this time an Internet emerged as a service.

II. Evolution of Cloud

The journey towards cloud computing is depicted in 3-phases as *Ideation Phase* during 1960- 90'which was an idea of computing as a utility computing and grid developed as shown in Fig. 3.

Since mid of 2000, it is assumed as the cloud phase which includes cloud computing and it becoming popular with the sub classification of IaaS, PaaS and SaaS got formalized as shown in Fig. 2.

According to envision of Cisco white paper-2009 the cloud computing is phased as a shown in the below Fig. 3. A private cloud path from an enterprise will begin very simply with a pilot deployment with target at mission support. Ex: highly variable workloads like development, testing training, demonstration labs in which it is highly advantageous for end users to self-provision systems and storage.

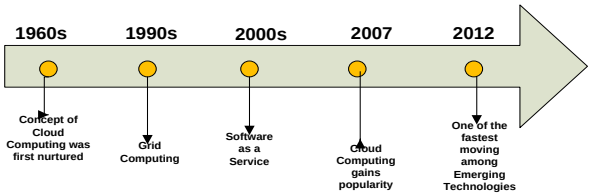

Fig. 2. Journey of cloud.

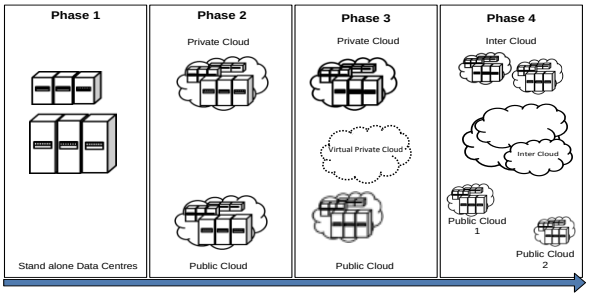

Fig. 3. Phases of cloud.

Other deployment cloud includes intranet applications that have widely varying loads as account systems, expense reporting. These pilots are typically very visible internally and are run in conjunctly with new or existing server and storage virtualization initiatives.

III. Challenges

In cloud computing there are yet many practical problems, which have to be solved. These unsolved problems are considered as the challenges and are found as follows:

A. Network Security

The network is main component for cloud that interconnects the systems in a cloud has to be Secure. The following will be the different challenges over the network.

B. Data Security

Confidentiality refers to those who stores the encrypted key-data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encrypt key. Integrity the face that no common policies exist for approved data exchanges; industry has different protocols used to push different software images for jobs. It involves encrypting the data as well as ensuring that appropriate policies are enforce for data sharing [10].

C. Virtualization Security

Virtualization paradigm in cloud computing results in several security concerns. Virtualization based on hypervisor, based on operating system (OS) and soon has to be concentrate on security of virtualization factor. Mapping the virtual machine to the physical machine has to be carried out securely. Security of memory and resource algorithm has to be improving towards the security of cloud. If the virtualization is based on the hypervisor, it is single point of failure because if attacker gets control over it, then he can get all VMs under his control. In operating system based virtualized cloud the attacker can inject his kernel script in hosting OS, by this he can run all guest OS on this kernel[11], [12].

D. Security of Memory

Resource allocation & management algorithm have to be improved to achieve the security of cloud computing.

E. Controlling the Sniffer Attacks

The sniffer program which runs through Network Interface Card (NIC) will ensure the data or traffic connected to the any other system on that network and if so gets recorded [13]. The NIC which will be in promiscuous mode can track all data following on the same network. The NIC will be placed in promiscuous mode and in promiscuous it can track all data following on the same network with help of Address Resolution Protocol (ARP) and Round Trip Time (RTT).

F. Internet Protocol (IP) Address Problem

Each node is attached with IP address issued recently if the present user quits the network, then that IP address associated to him/her assigned to new user, which is very dangerous as there is a certain time lag between the change of an IP address in Domain Name Server (DNS) and the clearing of that address in DNS caches. So, it can be concluded that sometimes through the old IP address is being assigned to a new user still the chances of accessing the data by some DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user [14]-[16]**.** With use of thin clients which run with as few resources as possible and do not store any user data like password and all cannot be steel the data.

G. Availability

Service provider has to aware of downtime along with contract polices between clients and vendors, so that data belongs to only to the clients at all times. He has to prevent third parties to be involved at any point [17].

H. Data Centre security

Data center related security issues involves physical access layouts of racks as well as servers example network redundancy and isolation, back up and disaster recovery contingency, intrusion detect and prevention systems etc., The infrastructure of data center is expected to have sensitive and critical customers to enter into public cloud. The cloud should meet the criteria listed below [18], [19] which are general security issues with the cloud computing and categorized into

1) Physical and software infrastructure security
2) The processing of data and its security

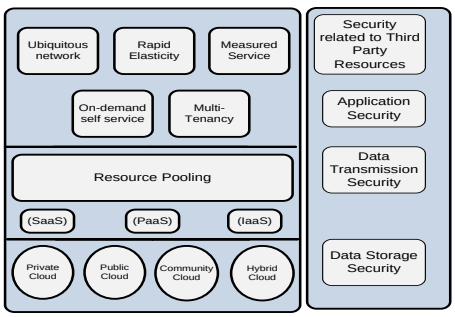

Fig. 4. Cloud environment security.

The shared vulnerability technology, which is required for the Hybrid PaaS and SaaS provides [20]. With common public key can be implemented. The cloud security is viewed from Fig. 4 which depicts the security of cloud at different level. Application Security is required at the level of ubiquitous network. In resource pooling with PaaS, SaaS, IaaS, data transmission security is required. For storing the data, based on type of deployment of cloud data security security essential.

The physical and software infrastructure security can be assured by solving or assuring

1) The security of data centers against the security breaches.
2) There must be potential common software stack of IaaS and PaaS to host the applicant with managing vulnerability.
3) Application interfaces and cloud providers interfaces must ensure security.

The security of processing of data can be achieved by integrity and preventing the loss of data in the cloud. The encryption mechanism like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) can solve this problem and also by holomorphic encryption [21], [22], which enables the cipher text to be processed in public cloud without and decrypting this will enables the user to possesses the private part of the key. With this key, the encrypted labels can be decrypted the data security and its processing can also be maintained by data confidentiality where multiple clouds are participate for processing of data can be managed with privacy preserving distributed data mining protocols which are listed in [23] "Classification of privacy preserving distributed data mining protocols" by Zhuojia XY, Xun Yi. The privacy preserving techniques may be of horizontal or vertical partition with any one of the techniques like Public-key encryption, oblivious transfer, randomization, secret sharing. Public key encryption should satisfy additive property

$$E(a) \times E(b) = E(a+b).$$

IV. Maintaining the Data from the Outside Word

It is very essential to maintain the some standards for security in cloud computing such as Security Assertion Markup Language (SAML) which is Extensible Markup Language (XML) based standard for communicating authentication, authorization and attribute information among online partners. The security transaction between partner organization regarding the identity and entitlements of a principal [24], [25] SAML is presently built on with standards like Simple Object Access Protocol (SOAP), Hypertext Transfer Protocol (HTTP) and XML.

For the authorization, open authentication can be used which is an open protocol initiated by Blaine Cook and Chris Messina for authorization of secured Application Program Interface (API). Open Identification (Open Id) can be used to identify the user and also to allow the access privileges it allows the user to log in once and gain access to resources across participating systems in cloud; provider can use this to identify their own users. The open Id protocol does not really a central authority to authenticate a user's identity. Neither the opened protocol nor any websites requiring identification can

mandate that a specific type of authentication be used, non-standard forms of authenticity such as smart cards, biometrics or ordinary password are allowed [26], [27].

The other security required is Transport Layer Security (TLS) as well as Secure Sockets Layer (SSL). SSL are the protocols for the photographic and can be used to design a secured and data integrated communication over TCP/IP network. TLS-SSL encrypts the segments of network connections at the transport layer. The protocol is meant for preventing eavesdropping tampering and message forgery [27]. TLS uses cryptography to provide end point authentication as well as data confidentiality. Here authenticity is one-way. The only server is authenticated; because the client remains unauthenticated.TLS also support mutual authentication[2] [24].These all works on Ethernets. We can change the network from Ethernet to advanced Optical Networks [ON].

V. Optical Network in Cloud

The old day's network and the present days network is Ethernet network. The some of the networks are adapted to optical network. In an optical network the information is passing through fiber channel and information to be passed is in the form of light. The fiber channel of optical network was Wavelength-division–multiplexing (WDM) and is adapted for many reasons, but now it switching to Dense Wave-Division-Multiplex (DWDM) which is under research for implementation for the optical network[28], [29]. The implementing of optical network with DWDM can also be limited to access network[3] for time being. The change of normal network to optical network leads to many changes in network and parts of the network also leading to expenses, but we can achieve secured speed of 100GBPS network, so if cloud computing is adapting optical network as its network for all the types of deployments then it will be very economic. Installation of ON is little bit expensive. In ON, for attackers it is difficult to get information like public key or private key, Deny of Services (DOS), eavesdropping vulnerability access as the information is interms of light.

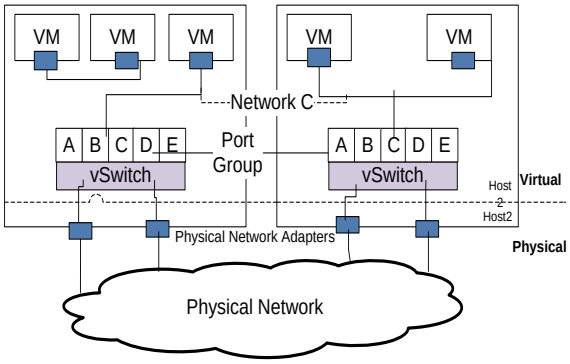

Fig. 5. Network architecture of optical network.

To have optical network it is very essential to have at least translucent network[4] [28]-[30]. Electrical /Optical switch which is a datacenter switch is replacing with HELIOS and MEMS (Micro-Electro Mechanical Systems) based optical circuit switch. The similar type optical devices can be used for the cloud computing's network to achieve the required security with higher speed.

According to VM White Paper-2009 [31], [32] the network architecture is shown as Fig. 5. In this architecture, we propose the optical based virtual machines and also physical network of optical network either transparent or translucent network the proposed network can overcome by all security problems with easy deployment as well as with faster ie up to 100 GPBS with Bit Error Rate (BER) as 10-12 to 10 -15 .

Virtual switches of network architectures of Fig. 5 are port group on one side. These port groups[5] connect to VMs. On other side are uplink connections to physical Ethernet adapters on the server where vSwitch resides. The shown architecture is rich set to provide virtual networking elements. These vSwitch can change to optical based switches. The VM can be of translucent type.

VI. Conclusion

Although Cloud computing can be seen as a new phenomenon, as an evolving paradigm, but has to set to revolutionise the present technology towards the potentialised technology for making it as next generation utility. There are yet many practical problems which have to be solved. Among the many problems to be solved, some of them are security concerns with virtualization based on hypervisor, based on operating system, IP address issue. Cloud computing is one of the disruptive technology with profound implications for Internet services as well as for IT sector as a whole. It is very essential to have highly secured cloud, if the cloud has a common security methodology then, it will be a high value asset target for hackers because of the fact that hacking the security system will make the entire cloud vulnerable to attack. This has to be much secured in all aspects by avoiding DOS, eavesdropping, hacking public key and private key with use of AES and DES methods along with some optical devices and optical network. The datacenters also have to maintain the security of processing of data, which can be achieved by integrity and preventing the loss of data in the cloud with advanced AES and DES methods.

Acknowledgment

The encouragement given by all faculties of Alliance College of Engineering and Design of Alliance University, Dean and stakeholders is highly acknowledged.

References

[1] GTSI, *White Paper on Cloud Computing Building a Framework for Successful Transition*.

[2] Mutual authentication: The unethically for both ends of the connecting to assure that commutating is between known user persons.

[3] Access network is the Public Switched Network (PSTN) that connects access nodes to individual subscribers which is passive twisted-pair cu-wire.

[4] Translucent Network: Optical networks, where some light paths are routed transparently, while others go through a number of regenerators, are known as translucent optical networks, i.e the type of optical network in which input and output to the node is in optical form where as processing is on electric form.

[5] Port group: It is a unique concept in the virtual environment. It is mechanism for setting policies that govern the network connected to it.

[2] F. Hao *et al.*, "Enhancing dynamic cloud based services using network virtualisation," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 1, January 2010.
[3] C. Y. Gong, J. Liu, Q. Zhang, H. T. Chen, and Z. H. Gong, "The characteristics of cloud computing," in *Proc. 39th International Conference on Parallel Processing Workshops*, 2010, pp. 275-279.
[4] D. Farber. Oracle's Ellison nails cloud computing. [Online]. Available: http://news.cnet.com/8301-13953_3-10052188.html.
[5] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," *Cryptography and Security*, vol. 2, 2013.
[6] A. Bakshi, B. Yogesh, and Dujodwala, "Securing cloud from DDoS attacks using intrusion detection system in virtual machine," in *Proc. the 2010 Second International Conference on Communication Software and Networks*, 2010, pp. 260-264.
[7] J. E. Dunn, "Spammers break Hotmail's CAPTCHA yet again," *Tech-World*, Feb 2009.
[8] Techworld News. [Online]. Available: http://news.techworld.com/?intcmp=ros-hd-nws
[9] Cisco Cloud Computing-Data Center Strategy, *Architecture and Solutions, Point of View White Paper for U.S. Public Sector Cisco*, 1st ed., 2009.
[10] R. L. Grossman, "The case for cloud computing," *IT Professional*, vol. 11, no. 2, pp. 23-27, 2009.
[11] V. T. Lam, Sivasankar, Radhakrishnan, A. Vahdat, and G. Varghese, "Netshare and stochistic: Predictable bandwidth allocation for data centres," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 3, July 2012.
[12] F. Sabahi, "Virtualization level security in cloud computing," in *Proc. 3rd IEEE International Conference on Communication Software and Networks*, 2011, pp. 250-254.
[13] N. Manohar "A survey on cloud computing- deployment of cloud, building a private cloud and simulators," in *Proc. ERCICA-2013*, pp. 408-4130.
[14] Z. Trabelsi, H. Rahmani, K. Kaouech, and M. Frikha, "Malicious sniffing system detection platform," in *Proc. the 2004 International Symposium on Applications and the Internet*, 2004, pp. 201-207.
[15] B. R. Kandukuri, R. V. Paturi, and A. Rakshit, "Cloud security issues," in *Proc. 2009 IEEE International Conference on Services Computing*, Bangalore, India, September 21-25, 2009, pp. 517-520.
[16] C. Wang, Q. Wang, K. Ren, and W. J. Lou, " Ensuring data storage security in cloud computing," in *Proc. 17th International workshop on Quality of Service*, USA, July 13-15, 2009, pp. 1-9.
[17] M. D. Dikaiakos and Dkali, "Cloud computing: Distributed internet computing for IT and scientific research," *IEEE Internet Computing Journal*, vol. 13, issue 5, pp. 10-13, September 2009.
[18] C. Balding. (2008). ITG2008 World Cloud Computing Summit. [Online]. Available: http://cloudsecurity.org/
[19] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud computing security-trends and research directions," in *Proc. 2011 IEEE World Congress on Services*, 2011, pp. 524-530.
[20] Telecommunication Industry Association. TIA-942: Data centre standards overview. [Online]. Available: http://tiaonline.org.
[21] Cloud security alliance. [Online]. Available: http://www.cloudsecurityalliance.org.
[22] IBM Homomorphic Encryption research page. [Online]. Available: http://domino.research.ibm.com/comm/research_projects.nsf/pages/security.homoenc.html.
[23] W. Stallings, *Network Security Essentials*, 3rd ed., Prentice Hall, July 29, 2006.
[24] Z. J. Xu and X. Yi, *Classification of Privacy Preserving Distributed Data Mining Protocols*, pp. 337-342.
[25] L. Ertaul, S. Singhal, and G. Saldamli, *Security Challenges in Cloud Computing*.
[26] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing Implementation, Management and Security*, CRC Press, August 17, 2009, pp. 147-158, 183-212.
[27] L. J. Zhang and Q. Zhou, "CCOA: Cloud computing open architecture," in *Proc. 2009 IEEE International Conference on Web Services*, 2009, pp. 607-615.
[28] Amazon White Paper. [Online]. Available: http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-centre-and-security-whitepaper/,published June2009.
[29] R. Ramaswami and K. Sivarajan, O*ptical Networks: A Practical Perspective. Morgan Kaufmann*, 3rd ed., 2009, ch. 3, pp. 114-237.
[30] N. Farrington, G. Porter, and S. Radhakrishnan *et al.*, "Helios: A hybrid electrical/optical switch architecture for modular data centres," *SIGCOMM'10*, vol. 40, issue 4, pp. 339-350, 2010.
[31] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: dynamic flow scheduling for data centre networks," in *Proc. NSDI'10*, 2010.
[32] *VM Ware Information Guide*, 2009.

Nivedita Manohar is working as an assistant professor in the Dept. of Computer Science and Engineering. Nivedita had completed her B.E in computer science and Engg. and M.Tech. degree in computer network engineering from Visvesvaraya Technical University Belguam, Karnataka, India. Her research interests are in the area of, cloud computing, and optical networks. She has many national and international publications in journals.