International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:12, 2014

Security Architecture for Cloud Networking: A Survey

Vishnu Pratap Singh Kirar

***Abstract*—**In the cloud computing hierarchy IaaS is the lowest layer, all other layers are built over it. Thus it is the most important layer of cloud and requisite more importance. Along with advantages IaaS faces some serious security related issue. Mainly Security focuses on Integrity, confidentiality and availability. Cloud computing facilitate to share the resources inside as well as outside of the cloud. On the other hand, cloud still not in the state to provide surety to 100% data security. Cloud provider must ensure that end user/client get a Quality of Service. In this report we describe possible aspects of cloud related security.

***Keywords*—**Cloud Computing, Cloud Networking, IaaS, PaaS, SaaS, Cloud Security.

I. Introduction

CLOUD computing is fastest growing area in the field of research and development. The computing industry has been changed in last decades, as it was based on centralized system in past i.e. client-server model but as the technology is advanced it become virtual centralized i.e. web base model. In simple words we can explain that cloud computing a technique that can provide services online over on Internet. In cloud computing service provider deliver various services and storage capacity as a service to end user or client.

Concept of cloud computing is an outcome of service model and deployment model. Services of cloud computing mainly categorized in three layers: Infrastructure as a service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These combine services form a service model for cloud computing. Similarly deployment mode for computing divided into the public cloud, private cloud and hybrid cloud. The cloud deployment can be explained in the relationship between user and enterprise, which provide the services. Public cloud services are sold to user for utility purpose, private cloud can be used by any organization for their datacenters; it is not for general user [1]. Thus cloud computing provide opportunities to small industries to outsource their services as they can built software's and applications online. These services are available as pay-as-you-go where user pay only for services and resources they actually use for a particular time period.

Clouds have different architectures based on the services that they provide to end user or client. The vendor of cloud stores their data in centralized location it is known as datacenter. The client does not know about the location of datacenter. Vendor only provides services and client only access the cloud services. Client does not have any control on datacenter. Communication between service provider and client is established only on Internet. Now Internet becomes a biggest platform for research and development of various emerging technologies.

Cloud computing is very efficient and very useful because it reduce the operating cost, maximize the utilization of resources and it is easy to use and easily accessible [2]. At the same time it is flexible and inexpensive to use the desired services. Thus, authenticity, indignity, availability, security and privacy are essential for cloud service provider and client.

Based on the service model IaaS is a basic layer of cloud computing and PaaS and SaaS are connecting and depending on it. Thus, overall Security of cloud depends upon IaaS layer.

In this paper we discus about security concern of IaaS layer i.e. what are the main challenges for security of IaaS and what are the solutions. The background of security of cloud computing and its layer will describe in Section II. The secondary research results are explained in Section III. The reflection of study provides in the Section IV. In last section we conclude our results and paper.

II. Background

In present scenario, various service providers on Internet are involved in development of their own cloud-computing environment for example Microsoft, Amazon and Google. Eric Schmidt from Google first introduce the concept of cloud computing. As we discus in first part cloud computing is combination of service model and deployment mode. Fig. 1 describe the cloud computing. The brokering goals of these layers are define in Table I.

A. Software as a Service

At this layer user can access the services that are provided by cloud service provider. These services include e-mail service, online antivirus, video chat and sharing. Most of the services are free.

B. Platform as a Service

PaaS provide a variety of services for developers. Developer does not require downloading any software. Vendor provides all resources. User can built any application, software, and perform the software testing. Example of PaaS is Facebook development.

C. Infrastructure as a Service

IaaS refers as a service provider; service provider performs the control of whole cloud. It can be access remotely. The service that provided by vendor may be paid or free, it depends on that service or tool.

Vishnu Pratap Singh Kirar is with the Computer Science Department, University of Bedfordshire, Luton, United Kingdom. (Phone: +44 7405400182; +91 9826020913; e-mail: Vishnu.kirar@study.beds.ac.uk).

Fig. 1 Cloud Computing Service Model

TABLE I
THE BROKERING GOAL OF SERVICE MODEL

Layer/Service	Parameter	Objectives
SaaS	User requirements	Maximum QoS delivered
	Service level agreement	Minimize cost
	Software Licensing	Functionality
PaaS	Compiling requirement	Functionality
	Runtime requirement	Optimize application
	Runtime licensing	Fault tolerance
IaaS	Resource characteristic	Maximize cost-effectiveness
	Monitoring data	Acceleration
	Modeling data	Conservation
	Constraints	Maximize energy efficiency

Services that provided by any cloud are clouds computing cloud storage, cloud operating system, cloud software and many more. Cloud provides a virtual interface between end user and vendor. The security related problem that faces by cloud system are mainly due to following reasons. Large amount of user data is stored in cloud. Nowadays personal data is valuable for many industries. Thus it is possible that third part may leak your information that stored in the cloud.VM architecture any one of the user can easily access the information of other user by using hacking tools. Because cloud is an open source thus there is need to implement some strict protocol on VM. Overload of traffic some time cloud may be crash or breakdown. Cloud has some limitation of accessibility if number of user increases at a particular time than cloud does not provide their services. Data storage security for user is main issue of security. Data must be secure so that user can access it when needed.

Cloud standard must be implemented on every system because if user wants to access more than one cloud than he can be easily accesses them without any interruption or any operating system dependency. Hence there is a need to build a standard for all cloud and they must follow them.

III. RELATED WORK

Cloud computing is facility of computing and storage capacity and it give a variety of choices along with many advantages to end-users. The cloud storage mainly divided into two classes: first cloud storage designed using cryptographic method but not follows the cryptography structure and second cloud storage design by follows the structure as well as method of cryptography. To secure cloud storage many researchers gave many proposals, which are based on cryptography [3]. Kamara et al. propose architecture by using non-standard cryptographic techniques. Barua et al. propose new scheme for cloud storage based on cipher text policy and encryption based on attribute as well as identity. Zarandioon et al. work on user-centric privacy preserving cryptographic access controlled protocol (K2C). Somorovsky et al. proposed a work on public cloud storage by introducing XML encryption.

Soel et al. propose a secure storage service for IaaS cloud users. They describe a model to secure the computing environment by using crypto-processors. To describe the solution they explain the VM [4]. VM consist mainly three objects: processing, memory and I/O. VM is secure until processing and memory is protected along with if there is no I/O operation is performed. But it is not an ideal condition because without I/O the existence of cloud is not use worthy. Hence, Soel et al. apply crypto-processors at I/O devices. Soel et al. explain the importance of hypervisor (a management OS) in VM. An attacker can get sensitive information via the management OS or direct access of dedicated privilege.

Soel et al. proposed some requirement for secure storage like isolated cryptographic operation, infrastructure cryptographic operation and key protection. They also suggest to place crypto-processor in the management OS. By using crypto-processors even cloud vendor cannot access the users information because the decrypted data are not in the domain of management OS.

At the present time thousand cloud servers put forward their services in different layer of software. But Hamid Banirostam et al. scrutinized lower layer of the cloud computing which called Infrastructure as a service (IaaS) and come across with the problem in it [5]. The problem is that who use the cloud computing they do not have privacy on their personal information or data. Because at this time, cloud computing do not offer any proper tool for user's verification of confidentiality, privacy policy, computer accuracy and data integrity. Because of that problem, Users' and companies' information or data are not secure. The major anxiety is to attack of privacy which may be internal or external. Attack on the information or data of a private company can affect its reputation

To overcome the problem of cloud computing Hamid Banirostam et al. bring a new approach called Trusted Cloud Computing Infrastructure inspired by Trusted Cloud Computing Platform. They suggest that information or data should be encrypted. So, to go with this approach and make a cloud computing more secure and trustworthy User Trusted Entity (UTE) is introduced by them and furthermore, the main benefit of User Trusted Entity (UTE) is that without permission of user, manager of Infrastructure as a Service (IaaS) system do not get in the way [6].

They also proposed about Trusted Computing Group (TCG). To build a trusted platform TCG has addressed a

number of hardware and software technologies. Standard for the chip of Trusted Platform Module (TPM) which is packed with hardware products that offered by TCG. The physical host would know some of the hidden action that is unchangeable because of TPM chip includes an Endorsement Private Key (EK). To make a remote verification potential Trusted Platforms build characteristics of TPM chips. They defined two components of cloud computing: Trusted VM Monitor (TVMM) and Trusted Coordinator (TC).

TVMM runs in every backend node of TCCI, which is the host of client. TVMM also look after to its information over time. TVMM also cooperate with TC in each node, which is running that includes: Limit a VM to a trusted node and protecting the position of VM against control or relocation while passing network in vital moments.

Cloud computing offers services at various levels such as SaaS, PaaS, and IaaS. These services include virtual resources provide service to within its limits [7]. For Example, network loading and security architecture. The main code of architecture is as cloud services to service users. According to services, it operated in a virtual machine like as Amazon's EC2, with in center of infrastructure. On the other hand, virtual resource is required a moving position for optimization issue because of security reasons flexible virtual resources creates new faces. When user moves to other network infrastructure track the services which user is a demand.

In the concept of Security Architecture, research shows some roles those are namely, Service User, Service Provider, Virtual Infrastructure provider and Virtual Resource [8]. All roles are interacting with each other such as service provider provides services to User. This service is only valid for authorized user. Service Provider connects services between User and a virtual Infrastructure Provider. It represent virtual IT and Provider used this information implementation services. Basically, the virtual infrastructure has an individual hardware, when it is turning on. Virtual Resource is unit of processing and data storing, which is, hold on physical resource of Provider.

In the case of Cloud computing, user wants to use security services it is based on policies. Nowadays, users verify safety parameters by using security requirements [9]. If provider replaces services then user checks manually requirements. Moreover, security parameter as a data encryption is in storing into security view. Security policy supports AES encryption methodology base on Key length. It implements into parameters of security side. In this subject, cost is main topic of infrastructure but it is not part of research.

IV. Reflection of Survey

Cloud computing overlaps with centralized, parallel and distributed computing. Cloud computing is a computing model, which is based on distributed computing, parallel, processing and virtualization and grid computing. As computing technology become more advance the risk of attack on information and security become at the first place. To guarantee a secure storage service, proposed architected by Soel et al. can easily achieve plain text isolation from the hypervisor and safe system state guarantee. Proposed technique by Soel et al. is very secure, it gives a choice to conventional user to switch from physical server to cloud server. Cloud is better option than physical server because it is cost effective, flexible and easy to use. As Soel et al. introduce crypto-processor for secure the storage services and they also state that they are working on to implement it on PCI device. If they are successfully implemented this device than these techniques can be implemented on other layers i.e. PaaS and SaaS. In my point of view the things that shoud be kept in account and which are very crucial, are the cost effectiveness and flexibility and maximum utilization [10]. So the system is very effective only when they apply the crypto-processor and the cost of system remain same or may be reduce.

The ideas that proposed by different authors and make a framework to implement cryptographic methods like AES because it is very secure method due to use of repetition rounds of encryption and decryption side. Also it is adopted all over in the world to the cost of implementation will be less as comparative to introduce a new method for security.

In the lower layer of the Infrastructure as a Service (IaaS) has some problem and cloud computing does not support any suitable tool for security. So, Hamid Banirostam et al. [5] introduce a TCCI approach to overcome that problem and for that UTE, TVMM, TC, TCG and EK all components or chip are very useful in plenty of way to put further functionality or secure privacy to make more attractive and trustworthy that is why this approach called Trusted Cloud Computing Infrastructure (TCCI). That approach inspired by Trusted Cloud Computing Platform. In addition to that, the main advantage for user through UTE is that the manager of IaaS has no privilege to interfere in Trusted Coordinator Functionality within UTE. Accordingly, cloud computing became an extra secure and more trustworthy by using these all approaches.

Cloud-networking architecture is displayed as security. As per the reason of scalable and movable virtual resources, registered users can access network at various virtual infrastructure in different time place [11]. The main thought of this research paper is security parameters, requirement and functionality, which is managing services by the service provide to the User and virtual infrastructure provider. In the near future, security architecture will be introduced in new face of verification user and providing flexible control via virtual resource in the cloud networking.

V. Conclusion

Cloud computing become a key research area due to its benefit like dynamic scalability, flexibility, rapid elasticity and seamless expansions. On the other hand due to integral security issues the evolution became restricted. The most vulnerable part of cloud computing is users data which is stored in the cloud. User cannot use cloud as a conventional method of storing the data. If cloud vendor provides enough security than user, it can move from server based storage to cloud base storage. The IaaS is the fundamental layer of cloud. If IaaS become more secure than whole cloud will be secure.

In this report we discuss various methods that are proposed by different authors. The most appropriate method that our group finds is to apply cryptographic method to secure the IaaS. Because cryptography can apply in all the fields of computing like software, applications, services and hardware as well. Hence proposed methods can be securing the whole cloud by applying it on infrastructure as a Service layer.

REFERENCES

[1] Seol, J.; Jin, S.; Maeng, S., "Secure Storage Service for IaaS Cloud Users," *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium*, pp.190-191, 13-16 May 2013.

[2] Yandong, Z,; Yongsheng, Z., "Cloud computing and cloud security challenges," *Information Technology in Medicine and Education (ITME), 2012 International Symposium*, vol.2, pp.1084,1088, 3-5 Aug. 2012

[3] Jog, M.; Madiajagan, M., "Cloud Computing: Exploring security design approaches in Infrastructure as a Service," *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International*, pp.156-159, 8-10 Dec. 2012

[4] Villegas, D.; Bobroff, N.; Rodero, I.; Delgado, J.; Liu, Y.; Devarakonda, A.; Fong, L.; Sadjadi, S.M.; Parashar, M.; "Cloud federation in a layered service model," Journal of Computer and System Sciences, Volume 78, Issue 5, Pages 1330-1344, September 2012

[5] Banirostam, H.; Hedayati, A.; Zadeh, A.K.; Shamsinezhad, E., "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure," *Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference*, pp.717-721, 10-12 April 2013

[6] Fusenig, V.; Sharma, A., "Security architecture for cloud networking," *Computing, Networking and Communications (ICNC), 2012 International Conference*, pp.45-49, Jan. 30 2012-Feb. 2 2012

[7] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A., "Cloud Security Issues," *Services Computing, 2009. SCC '09. IEEE International Conference*, pp.517-520, 21-25 Sept. 2009

[8] Peng, Y.; Zhao, W.; Xie, F.; Dai, Z.H.; Gao, Y.; Chen, D.G., "Secure cloud storage based on cryptographic techniques," The Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2, pp. 182-189, October 2012

[9] Dawoud, W.; Takouna, I.; Meinel, C., "Infrastructure as a service security: Challenges and solutions," *Informatics and Systems (INFOS), 2010 The 7th International Conference*, pp.1-8, 28-30 March 2010

[10] Gupta, S.; Satapathy, S.R.; Mehta, P.; Tripathy, A., "A secure and searchable data storage in Cloud computing," *Advance Computing Conference (IACC), 2013 IEEE 3rd International conference*, pp.106-109, 22-23 Feb. 2013

[11] Meera, A.; Swamynathan, S., "Agent based Resource Monitoring System in IaaS Cloud Environment," Procedia Technology, Volume 10, Pages 200-207, ISSN 2212-0173, 2013