Architecting the Network for the Cloud using Security Guidelines

K. Krishna Chaitanya
MVGR College of Engineering
Vizianagaram
Andhra Pradesh

ABSTRACT
Cloud computing is the latest emerging technology which offers reduced capital expenditure, complexity, operational risks, maintenance, and increased scalability while providing the services at different abstraction levels, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). A new approach called cloud networking that enables and adds the networking functions and resources to cloud computing and provide the means of dynamic and flexible placement of virtual resources that crossing over provider borders. It also allows various kinds of functionalities and optimization techniques, e.g., reducing network load. This approach brings out and enables new security challenges. This paper presents a new security architecture, which enables the user of cloud networking to illustrate the security requirements and apply them in the cloud networking infrastructure.

Keywords
Cloud Service Consumer; Cloud Service Provider; Virtual Infrastructure Provider; Cloud Service Creator; Virtual Resources.

1. INTRODUCTION
The cloud computing infrastructure is enabled in data centers. If a cloud service consumer orders a cloud service, e.g., a virtual machine in Amazon's EC2, these virtual resources are placed over the physical infrastructure within, data center of the cloud operator. The virtual resources may move within the data center from, one virtual machine to another one, e.g., due to maintenance reasons. A new transient system of one virtual resource to virtual machines in one data center of the same operator, or to other virtual machine of other operators automatically is not possible.

In cloud networking, the virtual resources are added to cloud computing, these resources are forwarded automatically from one operator's cloud infrastructure to another. Here, the security checks like data protection procedure are carried out automatically, to assure that an operator's infrastructure follows the cloud service consumer's demand. This approaches a cloud service consumer to define the security parameters and a virtual infrastructure provider can define its security functions. A cloud service provider checks the virtual resources, and maps them, and forwards the virtual resources of one virtual infrastructure provider to another virtual infrastructure provider.

The paper is organized along these lines. In this paper, individually introduces the architecture of cloud networking which will be used during the entire paper. In Section two, it shows the architecture of cloud networking and their roles (see section II).In section three, shows the cloud network security and growth of network forecast in cloud networking (see section III). In Section four, shows how the security functions are added to the cloud network architecture and define the functions that are needed to interact with architectural components with proposed model (see section IV). Afterwards, in Section five, defines the cloud network infrastructure and usage of cloud resources (see section V) .In section six, it gives an overview of related work (see section VI).In last (see section VII), section seven, it concludes the further working directions.

2. ARCHITECTURE OF CLOUD NETWORKING
In this section, personally introduces about the architecture for cloud networking [1] as shown in the figure 2.1, as used in this paper. This section consists of cloud service consumer, cloud service with virtual infrastructure provider, virtual infrastructure resources and. cloud service creator.

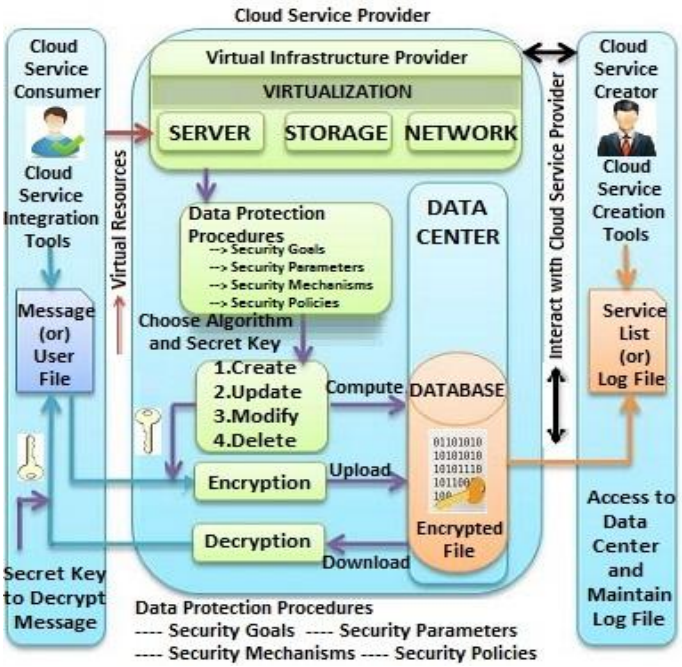

Figure 2.1. Architecture for Cloud Networking

2.1 Cloud service creator:

A cloud service creator is a person who is authorized to create the cloud services and assign the resources to the cloud service provider and to the cloud service consumer to use the cloud services by using administrative privileges. The cloud service creator maintains the service list or a log file containing all the resources carried out by a cloud service consumer by interacting with the data center and with a cloud service provider.

2.1.1 Cloud service creation tools:

A cloud service tool is one of the applications, which is used to create the cloud computational resources.

2.2 Cloud service provider:

A cloud service provider also called a virtual infrastructure provider is a person who is authorized to provide the services created by cloud service creator and assign the resources to service consumer to use the cloud services by the using virtual infrastructure. Cloud service provider manages the cloud infrastructure and cloud resources. The cloud service provider has also a function for requesting virtual resources. This function requests virtual resources to a virtual infrastructure provider. However, before sending the request to a virtual infrastructure provider the cloud service provider maps the security parameters of the cloud service consumer to the security parameters of a virtual infrastructure provider. The request contains the same overall goals as the request function from the cloud service consumer and additional security constraints which base on the security parameters of the cloud service consumer. The cloud service provider deliver the virtual resources after receiving the access to the virtual resources from the virtual infrastructure provider, and then cloud service provider forwards the access to the cloud service consumer.

2.2.1 Virtual infrastructure provider:

A virtual infrastructure provider under the cloud service provider is a person who is an authorized member, who can manage the cloud infrastructure containing different servers and storage devices and network infrastructure devices, using the resources by interacting with both the cloud service creator and cloud service consumer.

The virtual infrastructure provider offers his virtual resources and security functionality as security parameters to the cloud service provider. When the virtual infrastructure provider receives a request for virtual resources from a cloud service provider he invokes the virtual resources and mobilizes the requested security parameters. After having invoked the virtual resources and security parameters the virtual infrastructure provider sends the access to the virtual resources to the cloud service provider.

2.3 Virtual infrastructure:

A virtual infrastructure [4] is a platform that is provided and managed by a cloud service provider using virtual resources to use the cloud resources by a cloud service consumer. A virtual infrastructure consists of server virtualization to gain access the resources carried out by a user, storage virtualization to store the information and access to the resources by a user, network virtualization to manage cloud network infrastructure and access the resources by a user.

2.4 Cloud service consumer:

A cloud service consumer is a person who is authorized to use the services provided by the cloud service creator and the cloud service provider by using administrative privileges. Here, the cloud service consumer performs his functions to gain access cloud using the application with the help of cloud service providers using virtual infrastructure.

2.4.1 Cloud service integration tools:

A cloud service integration tool is one of the applications, which is used to gain access the cloud computational resources provided by the cloud service creator and cloud service provider through requesting for virtual resources. This request contains overall goals and type of resource, amount, and optimization parameters, and the security goals. The security goals are transmitted in form of security parameters. The translation of security goals to security parameters will be performed at the cloud service consumer side.

3. CLOUD NETWORK SECURITY AND FORECAST

3.1 Network Security in the Cloud

In this paper, the security plays a vital role to protect the information and the cloud from the security breaches, the cloud computing [5] follows all the data protection procedures like security goals, security parameters, security mechanisms, and security policies to protect the data and cloud from threats and data theft from unauthorized users. In this cloud networking architecture, the security is the key role that ensures to protect the information and cloud in a secure way, by following the data protection procedures and standards.

The primary goal of any information technology and security management [3] to protect information and system equipment without unnecessarily limiting access to authorized users and functions. IT security generally is composed of security goals, security parameters, security mechanisms, security policies and some security protocols, as shown in the figure 3.1.

Figure 3.1. Security Protocols in Cloud Computing

3.2 Growth of Cloud Computing and Cloud Network Forecast

Cloud computing is one of the latest emerging technology that mainly provides a useful option to IT field to reduce their complexity of usage and maintenance of their resources. Cloud computing provides an ensure quality of services to each organization and reduce the burden on their staff. It also enables higher levels of automation, deployment, orchestration, provisioning, and helps to their departments for more rapidly scale and their computational resources. In the

words of many organization executives study that cloud provides elasticity. International Data Corporation (IDC) is one of the organizations which are forecasting the growth of cloud computing over the next few years. In this IDC [2] survey the decision makers found that a few organizations are "considering only private clouds", which helps the user interest in the cloud technology and their early stages of cloud adoption. IDC expects about the cloud network infrastructure, which invests more double over the next few years, growing over $1 billion in each by 2013 for the public cloud and private cloud usage. Here, the cloud computing usage and worldwide public cloud and private cloud network forecast, as shown in the figure 3.2, of few years from 2009 to 2015, enabling the resources by the cloud based services providers on the data center network equipment.

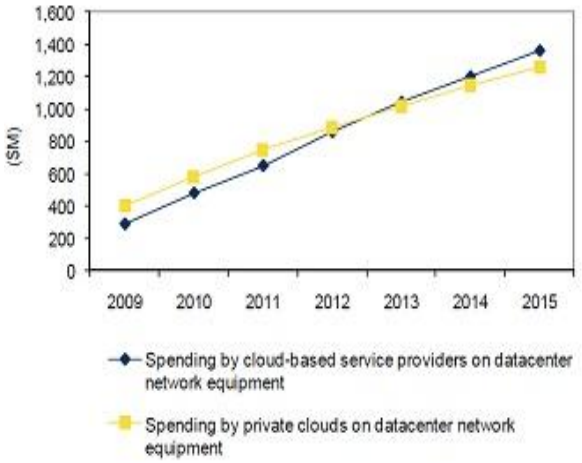

Figure 3.2. Worldwide Public Cloud and Private Cloud Network Forecast (2009-2015)

4. SECURITY FUNCTIONAL APPROACH FOR PROPOSED MODEL

In the proposed model of security functional approach, as shown in the figure 4.1, the user performs their roles and responsibilities to gain access to the cloud resources using the virtualization mechanism, by requesting resources to cloud service provider, the cloud service provider forwards user request to the virtual infrastructure provider, by invoking the resources from the virtual infrastructure provider, the cloud service provider deliver the resources to the cloud service consumer, thereafter user follows cloud data protection schemes and performs data protection procedures, user choose the algorithm and secret key to encrypt the message and upload it to data center and in the same way user download his message from data center and choose the same algorithm and secret key to decrypt his/her message and access to the data center to perform his functions using data protection procedures. Cloud service provider provides security functions to cloud service consumer to allow access to cloud resources and maintain the cloud created by cloud service creator and manages the cloud using the cloud privacy protection scheme [6] and other resources. Using virtual infrastructure provider a cloud service provider manage the cloud using server virtualization to allow access to cloud resources and storage virtualization to allow access to the database and network virtualization to manage the cloud using virtual resources. Cloud service creator allows user to gain access the cloud resources with the help of cloud service providers and interact to data center and with cloud service provider to maintain the log file (or) service list of a user, to manage his/her security functions.

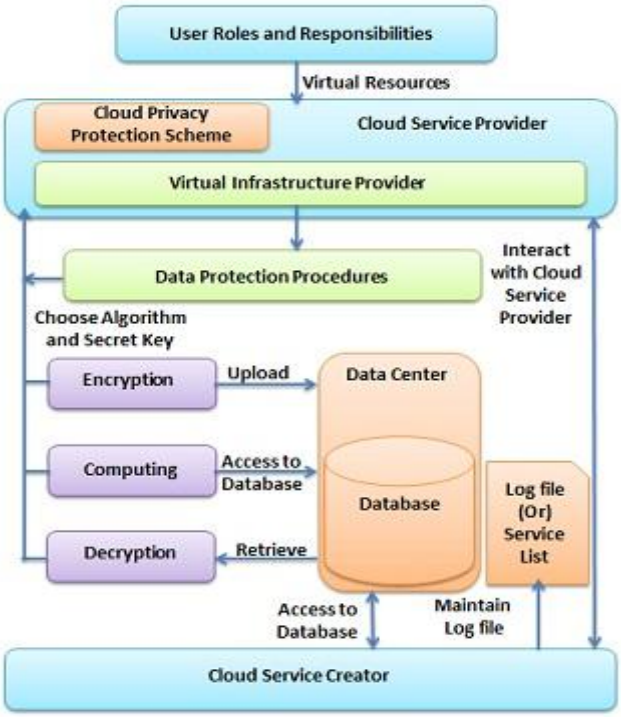

Figure 4.1. Security Functional Approach for Proposed Model

4.1 AES in the cloud:

Advances Encryption Standards is one of the security algorithms, which provide the security for the user information. Cloud Service Provider provides this encryption mechanism in the cloud, as shown in the figure 4.2, based on their virtual infrastructure provider resources. When a user chooses the cloud, the service provider forwards the user request to the virtual infrastructure provider and thereafter user uploads his/her file to the cloud based on the security policies. In this, the cloud provides security to the user data by encrypting the data based on AES algorithm by choosing the random key automatically, and provides the secret key to the user; this secret key is useful to the user to download his/her data or file from the cloud.

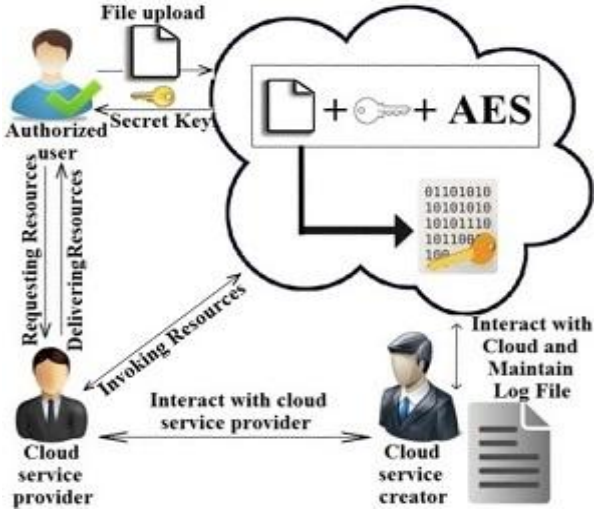

Figure 4.2. AES operation in the cloud

4.2 DES in the cloud:

Data Encryption Standards is one of the security algorithms, which provide the security for the user information. Cloud Service Provider provides this encryption mechanism in the cloud, as shown in the figure 4.3, based on their virtual infrastructure provider resources. When a user chooses the cloud, the service provider forwards the user request to the virtual infrastructure provider and thereafter user uploads his/her file to the cloud based on the security policies. In this, the cloud provides security to the user data by encrypting the data based on DES algorithm by choosing the random key automatically, and provides the secret key to the user; this secret key is useful to the user to download his/her data or file from the cloud.

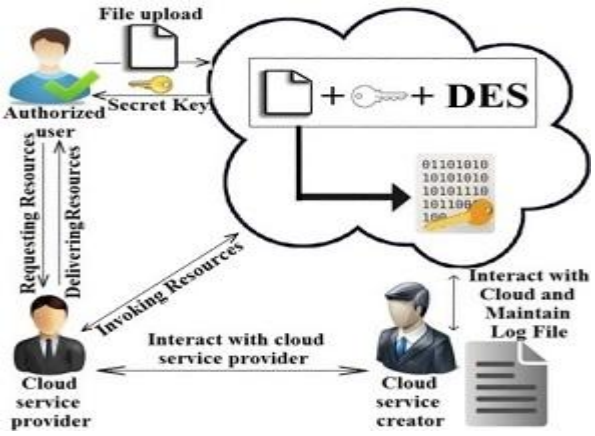

Figure 4.3. DES operation in the cloud

4.3 FILEKEY operation in the cloud:

Filekey function is one of the security functions, which provide the security for the user information. Cloud Service Provider provides this encryption mechanism in the cloud, as shown in the figure 4.4, based on their virtual infrastructure provider resources. When a user chooses the cloud, the service provider forwards the user request to the virtual infrastructure provider and thereafter user uploads his/her file to the cloud based on the security policies. In this, the cloud provides security to the user data by encrypting the file based on Filekey function by choosing the random key automatically, and provides the secret key to the user; this secret key is useful to the user to download his/her data or file from the cloud.

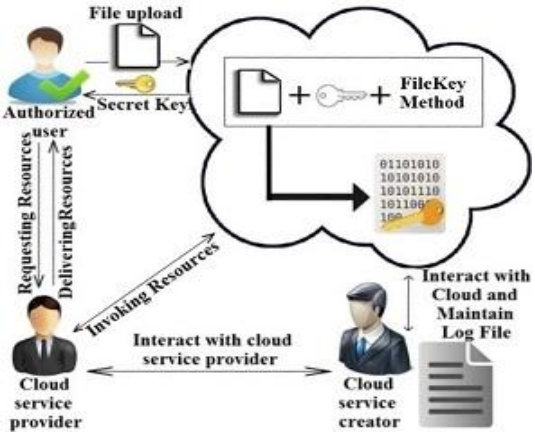

Figure 4.4. Filekey operation in the cloud

5. CLOUD INFRASTRUCTURE AND USAGE

In this proposed model of cloud networking [8], the cloud is designed in a way to protect the data and information of a cloud service consumer in a secure way.

5.1 Infrastructure:

Cloud infrastructure is designed in a secure way to protect data confidentially from unauthorized users. The cloud resources are designed using the virtualization system like XEN to gain access to the cloud resources. One virtual infrastructure provider offers 20 Gb of storage system with different algorithms like AES to store data in an encrypted format and another virtual infrastructure provider offers 40 Gb of storage system with different algorithm like DES to store data in an encrypted format, these virtual infrastructure providers moves/forwards their resources from one virtual infrastructure provider to another virtual infrastructure provider, if the resources are suitable based on cloud service consumer request.

5.2 Usage:

When a new cloud service consumer wants to access the cloud, he/she has to register/sign-up with his details and maintains his credentials in a secure manner. When a cloud service consumer wants to upload his confidential information in a cloud, he will choose the cloud and virtual infrastructure provider first and gain access to cloud resources by requesting the resources to cloud service provider to perform his/her operations and thereafter he has to provide his credentials to upload the file, the cloud service provider stores the information in the cloud [9] in encrypted format and provides the secret key to cloud service consumer to access his file after each file upload. This secret key is useful to the cloud service consumer to gain access to his/her files in the cloud to make changes and to download the files from the cloud. The files are stored in a data center of cloud resources in a secure way in encrypted format based on the algorithm chosen by the cloud service consumer, these data centers follows different algorithms to protect the data e.g., one virtual infrastructure provider follows AES and another virtual infrastructure provide follows DES and so on.

6. RELATED WORK

As cloud networking is a new research topic performed by many organizations, in this the main work is related to the security in this field. There are many data protection procedures that prove how to enforce security in cloud computing, e.g., secure selective sharing of resources based on new encryption schemes and proposes a security management framework. This framework is only for a single provider and is not applicable to a multi-provider. In this approach there is a flexible distribution of virtual resources are needed for cloud networking. The basis for virtualization as used in cloud infrastructures are for example VMware [7]. Here, cloud networking also needs the access to the networking resources through network virtualization techniques is also needed. Virtualization techniques and hardware acceleration techniques become important when building the security architecture.

7. CONCLUSION

In this paper, it concludes the security architecture for cloud networking. This architecture helps in preserving the security goals of cloud service consumers while at the same time benefiting from the flexible and dynamic placement of virtual resources at different virtual infrastructure providers. The main concept of this architecture is the definition of unique security and data protection procedures and standards, and the management of cloud service consumers and virtual infrastructure providers by cloud service providers. In further steps it plan to include the data protection procedures in a reliable and secure way and also plan to extend the architecture by auditing techniques so that a cloud service consumer and a cloud service provider are able to verify that security constraints that are followed by a virtual infrastructure provider.

8. ACKNOWLEDGEMENT

My sincere thanks to Dr. Sumit Gupta, Head of the Department of Computer Science and Engineering and to Mr.P.Ravi Kiran Varma, Coordinator of M.Tech CNIS branch, CSE Department to provide this opportunity to do the project under the guidance of Mr.P.Srinivas rao, Sr.Assistant Professor for guiding me for this project in each and every step and would like to thank to College management and everyone who helped me guiding the project.

9. REFERENCES

[1] Volker Fusenig and Ayush Sharma (2012) "Security Architecture for Cloud Networking" International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium 978-1-4673-0009-4/12.

[2] Lucinda Borovick and Rohit Mehra, IDC White paper "Architecting the Network for the Cloud," Cisco Systems, January 2011.

[3] "ISO/IEC 27001:500 - Information security management systems - Requirements," July 2011. [Online]. Available: http://www.iso.org/iso/ catalogue detail?csnumber=42103

[4] G. P. Koslovski and P. V.-B. Primet, "Vxdl: Virtual resources and interconnection networks description language," Engineering, pp. 138–154, 2009.[Online].Available:http://www.springerlink.com/index/N131016226414516.pdf

[5] A.Streitberger, W.Ruppel, "Cloud computing security – protection goals, taxonomy, market review," Institute for Secure Information TechnologySIT, Tech.Rep., 2010.

[6] S. D. C. d. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Encryption-based policy enforcement for cloud storage," in Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, ser. ICDCSW '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 42–51. [Online]. Available: http://dx.doi.org/10.1109/ICDCSW.2010.35

[7] "VMware," July 2011. [Online]. Available: http://www.vmware.com

[8] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for cloud networking security," in Mobile Networks and Management, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, 2010.

[9] "CloudAudit: A6 - The Automated Audit, Assertion, Assessment, and Assurance API ," July 2011. [Online]. Available: http://cloudaudit.org