RESEARCH ARTICLE OPEN ACCESS

A Survey On Cloud Networking

Prof.Gaurav Buddhawar, Mr.Ketan Belekar
[1]Department of Computer Science and Technology Namdeorao Poreddiwar College of engineering and Technology,Gadchiroli
[2]Department of Computer Science and Technology University of Bedfordshire,U.K

Abstract
Cloud computing is one of the evolving technology in today's era. It has changed the whole view that distributed computing, grid computing and parallel computing used to present. In the past few years cloud computing has grown widely and becomes the part of the IT industry, because it offers reliability, scalability, flexibility and cost effectiveness for computer processes. And also it offers reduced capital expenditure, complexity and maintenance, operational risks to those who ask for the service. It provides economical computing resources for business applications to small, medium and large organizations. It offers the resources and services through internet, where these services are delivered form data centres located throughout the world. Cloud networking is a new approach which adds networking functionalities to the cloud computing. It extends the approach of cloud computing by providing extra flexibility in the aspect of location, movement and interconnection in between virtual resources. This paper surveys the concept of cloud networking, cloud network management and its security architecture.

Keywords- Cloud computing, Cloud Networking, Network Virtualisation, cloud networking security

I. INTRODUCTION

In cloud computing, provider offers various services to the user through internet from anywhere at any time across the globe. It can be viewed as virtual pool of computing resources (e.g., networks, servers, storage, applications, and services) that are accessed through internet. It is the next generation of networking computing which can deliver software and hardware as on-demand services and resources with low cost and complexities [1-2]. Most of the organisations such as Google, Amazon, Microsoft, Oracle and HP are working on it to provide cloud solution in several ways. The cloud provides three major types of services in cloud environment: Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [3-4].

SaaS- Software's are provided as a service to the users which enable consumers to use the service on cloud server without installing the software in their local machine. (e.g. GoogleDocs [5]).

PaaS- In this platform is provided to the users, which enables them to develop new applications or services and also put their customized software's and applications on cloud. (e.g. Google's AppEngine [6]).

Iaas- It provides ideal environment for running applications. Storage, hardware, servers, and network component are provided in this, which enables users to manage applications, storage, operating system and network. (e.g. Amazon's EC2 [7]). It is also known as Hardware as a service (HaaS).

There are four types of clouds in cloud environments: Public cloud, Private cloud, Hybrid cloud and Community cloud [8]. Public cloud is accessible to any user, which offers several resources such as storage and applications to the public (any user). Private cloud is maintained by individual organization. Employees of that organization in private cloud have access to the cloud services. Hybrid cloud is the combination of one or more clouds (public, private and community clouds). In hybrid cloud, the cloud services are accessible to the organization users and also to the authorized public users. Community cloud is mixture of one or more clouds (public, private, and community cloud). In community cloud, the cloud services are shared by many organizations or within community for single reason. Cloud computing helps many organizations to store and process their huge amount of data efficiently with minimum cost and flexibility over the internet.

"The concept of cloud networking extends cloud computing in a way that it allows extra flexibility in placement, movement, and interconnection of virtual resources" [9]. The project SAIL (Scalable Adaptive Internet Solutions) [10] investigates cloud networking as the combination of cloud computing infrastructures and network infrastructures. In cloud networking, networks can easily be reconfigured within cloud environment. In this virtual resources are connected and moved automatically from one operator's infrastructure side to another. Cloud applications demands for a flexible network, because of this virtual resource can be placed in order to minimize latency of access and network load. This paper presents an architecture developed in SAIL that supports virtual infrastructure deployed on-demand through multiple providers, including data centre and network operators.

This paper is organized as follows. Section II presents the concept of cloud computing to cloud networking. Section III describes the cloud networking architecture. Section IV explores the Network management. Section V presents security architecture for cloud networking. The last section VI concludes and shows future work directions.

II. Cloud Computing to Cloud Networking

Cloud computing is growing widely in the field of computing and communications. Cloud computing is seeking the attention of many industries, network operator, and service providers are attracted towards cloud computing. This happens due to the introduction of infrastructure virtualization [11]. The separation of service provider from infrastructure providers reduces the operational and capital expenditure and financial risk to the service provider. And it gives opportunity to build large infrastructure which is beneficial from economics scale to the infrastructure provider.

A. Virtualization in Cloud Computing

Virtualization is the key feature of cloud computing. Its main purpose is to improve the server performance by providing virtual machine with an operating system (hypervisor such as Xen [11] or VMware [12]) to the user. It has become the ultimate technology in cloud computing that enables cloud computing platforms to dynamically allocate virtual machines as internet services. The current IaaS is made on server virtualization, network virtualization, and storage virtualization. Virtual machines, network and data storage are positioned and managed by data centre management in order to construct infrastructure topology. Large data centre placed near to low cost power, land and effort provides low cost to the provider. In order to reduce the load, transfer lost and damage to the services, each data centre is located at multiple geographical locations which are near to the users. The connection in between the data centre and IaaS user is handled by the open Internet [13]. This flexible placement of virtual resources can create many concerns to the user and provider like; user connectivity to the data centre, availability of services. To overcome this IaaS providers have added VPN tunnelling connectivity (Amazon Virtual Private Cloud [14]). The IaaS business model is shown in the figure 1.

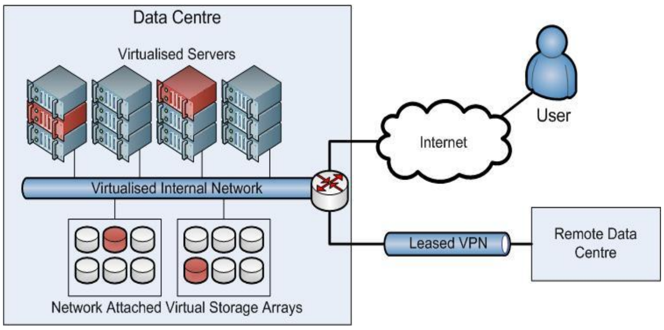

Figure 1: cloud physical infrastructure architecture [13].

B. Virtualization in Cloud Networking

Network virtualization is one of the great achievements for cloud computing environment. With the help of virtualization provider can create a new virtual network as per customer requirements (like bandwidth, protocols, security and end-to-end delay). It also brings the other benefits such as re-configuring the network in real time without dropping the connectivity, change in physical path, and moving one or more virtual nodes form one place to another [13]. Cloud networking can able to connect the user in the cloud and interconnect services that are geographically distributed across cloud infrastructures [8]. The users can specify their needed virtual infrastructure and desired network properties to access the resources through a single control interface. The figure1 is transformed and shown as follow in figure 2.

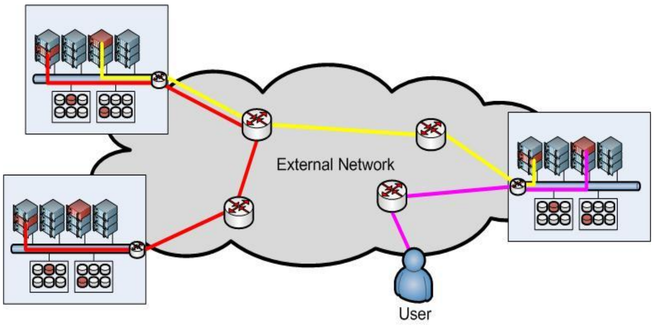

Figure 2: dynamic virtual networks connecting to distributed service [13].

C. Concept of Cloud Networking

Cloud networking is introduced to change the present image of cloud computing in network aspect. It is introduced in a multi-administrative domain scenario where network and data centre exists in cloud networking and these must interact with each other through defined interfaces to provide a service to the consumer. “Cloud networking service is adaptive, scalable, reliable, autonomous and operates seamlessly” [15]. These features demands cloud networking architecture to be efficient in specifying services, fast deployment and management of services across network operator and data centre, and providing and maintaining the quality of service.

The main concept of cloud networking architecture is combination of virtual networks across data centre and network operator infrastructures and positioning of storage resources across network operator. Flash Network slice (FNS) [10] is a new component of virtual infrastructure which is introduced in cloud networking in order to exploit these infrastructures. It is created and managed with in single administrative domain. It can be attached to the resources by links through which it forwards the messages in between them.

III. CLOUD NETWORKING ARCHITECTURE

The architecture of cloud networking provides scalable and efficient management of computational, storage and network resources. Cloud networking architecture is designed to overcome the cloud computing challenges such as; Multi-domain operation, Scalability, Heterogeneity, Dynamic provisioning and reconfiguration, Robustness and security [16]. The high level architecture for cloud networking is mainly divided into four parts; three layer model, set of roles, set of interfaces and set of management functions. These above three are characterised with reference to three layer model. The three layer model consists of resources, single-domain infrastructure, and cross-domain infrastructure [16]. The cloud networking architecture is depicted in figure 3.

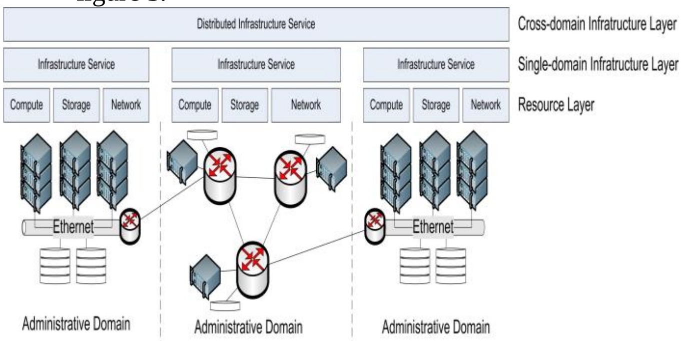

Figure 3: The three layer model for cloud networking [16].

C. Resources

A virtual resource retains within the boundary of single-administrative domain. This layer includes compute, network and storage resources as a virtual entity [17]. The virtual resource can be created, managed and destroyed by a subsystem such as the management interface on virtual machine hypervisor [16]. While creating a new virtual resource, it acquires some physical resource like disk space and logical resource like Internet Protocol. It has certain properties and status. The property (externally determined) of virtual resource is like memory size of virtual machine or address space for subnet and status (internally determined) is like condition of resource. Cloud networking suggests the computing and storage resources to be positioned in the operators network. Virtual resource have link to the other resources, a link describes a relationship in between them. A virtual machine manager may have to connect to the network or the storage device within the network. The virtual resource can be managed by single administrative domain, and it may have link to the other virtual resources in other administrative domain.

D. Single-Domain Infrastructure

A single-domain infrastructure consists of number of virtual resources that are managed together within a single administrative domain. It is managed by a single person who has right by management or administrative authority that has right over underlying equipment and virtualization technology [9]. With this a single administrative authority has complete knowledge about resources and virtualization capability. The mapping of virtual resources can be done at this level (e.g. placement of virtual machine in order to achieve the network performance) [16]. Single-domain infrastructure can be created, managed, updated and deleted.

E. Cross-Domain Infrastructure

A cross-domain infrastructure consists of number of virtual resources that are managed together within a multiple administrative domain. It can be partitioned into multiple single-domain infrastructures. It is managed by multiple administrative authorities. In this the underlying equipment and virtualization capabilities are not fully shared beyond domain boundaries. Decomposition of the virtual infrastructure into administrative domains is performed at this level. Cross-domain infrastructure can be created, managed, updated and deleted.

F. Roles

In cloud networking architecture three common roles are given such as administrator, infrastructure user and infrastructure provider [15]. Administrator has power to create and manage the virtual infrastructure in administrative domain. The administrator has control over physical or virtual equipment. Infrastructure service user can access an infrastructure service to find, scan, modify and destroy resources. Infrastructure service provider offers services to the infrastructure service user.

G. Interfaces

The three interfaces are resource administrator interface, distributed control plane and infrastructure service interface [16].

Resource administrator: This interface is used by administrator role to create, manage and destroy the virtual resources within an administrative domain. This interface is an implementation specific and it must provide the information of network topology and technology used, so administrator has to decide how to manage resources and what information is passed through these interfaces. Compute, storage or network resource interface provides specific information to the administrator which then used specifically to configure the resources as per user's need. Computer resource interface provides creation, deletion, start, and stop of virtual machines. It computes the service query and configures the compute service characteristics. Storage resource interface is mainly rely on standards like cloud data management interface. Because of this it is widely accepted in cloud. Network providers offer storage space to user for storing cache, files and documents. Network resource interface are introduced in cloud networking to configure, and manage the network as a part of cloud environment [19].

Distributed Control Plane: It is a collection of interfaces, protocols and control operations. It is used by infrastructure providers to communicate and exchange cross-domain information. The protocol and interfaces may vary; it depends on the relationship between domain and technology used. The interactions which take place in between the providers are reference solution, notification and distributed information sharing. It operates at cross-domain infrastructure level and is responsible for distributed coordination and global information access.

Infrastructure Service: It is the major part of cloud networking architecture. It consists of set of interfaces through which infrastructure service user can create, monitor and manage virtual infrastructure provided by infrastructure service provider [17]. Its main objective is to allow the user to specify high level goals in the form of system level service which then broken into low level control actions. It requires well-defined security model to fulfil the security constraint.

This arrangement is shown in figure 4.

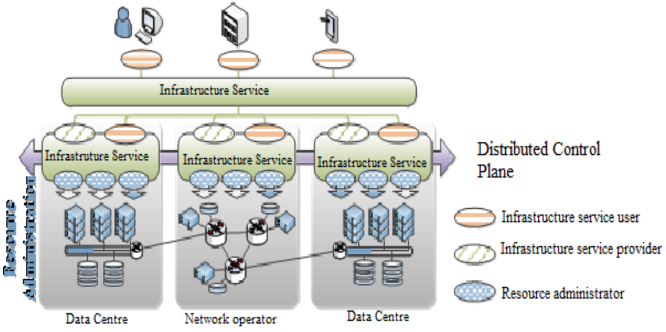

Figure 4: Interfaces of cloud networking [15].

IV. CLOUD NETWORK MANAGEMENT

In order to achieve the efficiency and flexibility for the virtual resource usage, the management solutions are designed in efficient, scalable, adaptive and autonomous manner [18]. It should provide the effective management for computational, network and storage resources. The management functions work within infrastructure provider and contribute in handling administrative domain. The management functions exchange information through the distributed control plane and management functions interfaces in both single and cross domains. The architecture of cloud networking management is basically consists of three management functions: goal translation, fault management, and resource management. This arrangement is shown in figure 5.

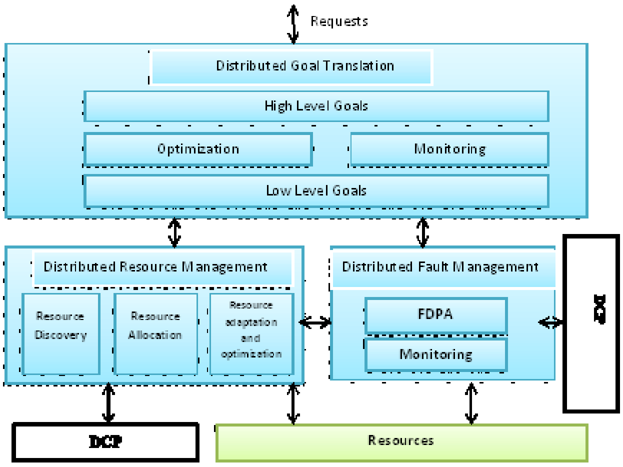

Figure5. Conceptual view of Management Architecture

H. Goal translation

The goal translation is used for transformation of high-level objectives like business, technical and security goals into the resource configuration objective. Through this user from different background with different motives can request and manage the services without dealing with low-level configuration services. It has three main responsibilities such as which service to accept, translate the service into low-level objectives, and control the high and low level objective. Goal translation function consists of four functional blocks: high-level objectives, optimization, monitoring, and low-level objectives. The high-level objective block is accountable for collecting and handling the high-level objective from infrastructure service interface. The optimization is responsible for finding a solution suggested by resource management into low-level objectives which is similar to the high-level objectives. The monitoring block is responsible for the requirement of low-level objective. The low-level block contains the translated objectives.

I. Fault Management

The fault management function gives the status updates of resources, measurements and models. It also monitors the performance of resources, resource management, security mechanisms, infrastructure service providers and users. It detects faults and change in the monitored resources. The fault management function encloses a Fault Detection and Performance Analysis (FDPA) block, which is responsible for the implementation of algorithms and a monitor block for the measurement of resources [16]. The FDPA is responsible for analysing and displaying the resource behaviour, and can also monitor the management functions. The distributed knowledge plane (DKP) can be considered as high-level abstraction of distributed information which is accountable for exchange of fault management information between providers. It represents distributed information recovery and maintenance information of distributed resources. DKP gives information transparency over the equipment on which management functions operates. The DKP can be related to databases or recovery information or information of networks.

J. Resource Management

The resource management is accountable for provision, allocation, optimization, and reconfiguration of resources. It records the properties of resources within management scope. Resource management gives the information about possible solutions to the low-level objectives. These solutions may include the cost or performance. The resource management offers the collecting of multiple resources, allocation and de-allocation, and optimization of resources. It also manages the workload and traffic among resources. It consists three types of blocks; resource discovery, resource allocation, and resource adaptation and optimization. The resource discovery is responsible for providing topology information and characteristics of resources. Resource allocation allocates and configures virtual resources. Resource adaptation and optimization block adapts and re-optimises the use of resources on periodic basis.

V. SECURITY ARCHITECTURE FOR CLOUD NETWORKING

As the cloud networking arises it introduces so many security challenges which affects the accessibility, reliability, confidentiality, authenticity and privacy [20]. Because of the flexibility and distributed nature of cloud networking it demands for the new security solutions. In order to make the secured networking architecture, availability, integrity, confidentiality, authenticity, privacy and non – repudiation are some factor one should consider [20].

Availability: Availability is measurable quantity, it is used to measure the parameters such as; response time, number of user served in parallel and bandwidth. It means the system is not in a condition to deliver service to the user. In cloud networking it means the unauthorized user can’t manage the services.

Integrity: In cloud networking, it means the system cannot alter the data without authorization. Integrity of data and communication are the important, while accessing and providing services.

Confidentiality: It means the system cannot access the data without authorization. The user should have the proper rights assigned by the provider to access the resources on cloud networking. It needs some specific tools to manage.

Authenticity: It is needed in cloud networking to verify the user and provider. It is used for verifying the user on network. It is also useful for the user on the cloud networking infrastructure, so that the users can verify to which infrastructure service they using or accessing.

Privacy: Privacy is very important for both user and provider. A subject is able to decide which information or what service wants to share. In cloud networking a user can share limited amount of personal information, it’s up to user wish, and provider can share the necessary information on the network.

Non-Repudiation: It is similar to traceability; it is used to track the location of infrastructure.

There are some security challenges [16] in cloud networking which are discussed below.

Information Security is one of main concern in the cloud networking because data is stored and managed on the cloud networking infrastructure. To ensure the security of data providers offer encryption of data to improve the confidentiality and integrity. The provider defines the security policies at infrastructure side and user should have to follow that policies. Virtualisation Management is like management of virtual infrastructure on cloud networking. Managing the virtual infrastructure on networking is a challenge to provider, so provider must maintain it. Misuse protection is similar to cloud computing, the virtual infrastructure can be misused (spamming, sniffing) by anyone so provider should provide the defence mechanisms to protect it. Denials of service attacks are common in computing, and it happens in cloud networking also. Its effect is higher as compared to other security challenges. The security architecture should provide the some defence mechanisms against DoS attacks.

The security architecture in cloud networking plays a vital role, in order to provide better security mechanism the architecture should ensure the security of each and every providers, consumers and operators. The architecture is designed in such a way that the security goal must be categorized to each specific resource. For every user there must be a group of security parameter, these then represented on to resource constraints. Provider should assign the security parameter in order to satisfy the user specification or requirement.

VI. CONCLUSION

This paper shows the cloud networking concept and its architecture which was presented in the project SAIL. And also it reflects the management and security mechanism for the cloud networking. This architecture brings the infrastructure provider and user a new way of accessing and managing the virtual infrastructure service in a secured way. It introduces the concept of managing and processing the resources at real time and also it gives a new way of dealing with network issues. It allows user to measure the performance of the virtual resources distributed in the infrastructure. It offers the security mechanism through which infrastructure service users and providers can create their own policies and manage the security at their own level.

This architecture is under development so in future there will be so many changes are going to happen in it. The flash network slice is introduced to the cloud networking as network resource type. The cloud networking shows the real-world applicability on interfaces and multiple models in the networking technology.

REFERENCES

[1] M. P. Rad, A. S. Badashian, G. Meydanipour, M. A. Delcheh, M. Alipour, and H. Afzali, 2009, "A Survey of Cloud Platforms and Their Future," IEEE Computer society, 8.

[2] H. Wu, C. Winer, L. Yao, Y. Ding, 2010, "Network Security for Virtual Machine in Cloud Computing," IEEE Computer Society, 4.

[3] F. Sabahi, 2011, "Cloud Computing Security threats and responses," IEEE Computer Society, 5.

[4] M. Carroll, A. V. D. Merwe, P. Kotze, 2011, "Secure Cloud Computing" IEEE Computer Society, 9.

[5] "Google Docs," 2011, http://docs.google.com accessed on 15/11/2012.

[6] "Google App Engine," 2011, http://code.google.com/appengine accessed on 15/11/2012.

[7]" Amazon Virtual Private Cloud," 2011, http://aws.amazon.com/ec2/ accessed on 16/11/2012.

[8] T. Ries, V. Fusenig, C. Vilbois, T. Engel, 2011,"Verification of Data Location in Cloud Networking," IEEE Computer Society, 6.

[9] J. Panneerselvam, L. Liu, R. Hill, Y. Zhan, W. Liu, 2012, "An Investigation of the effect of Cloud Computing on Network Management," IEEE Computer Society, 6.

[10] SAIL Project Website, 2011, http://sail-project.eu acessed on 18/11/2012.

[11] P. Braham, B. Dragovic, K. Fraser, S. Hand, T. Haris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, 2003, "Xen and Art of Virtualization," Google Scholar, 14.

[12] VMware, http://www.vmware.com.

[13] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, D. Zeghlache, 2010, "Challenges for Cloud Networking Security," Google Scholar, 17.

[14] Amazon Virtual Private Cloud, 2012, http://aws.amazon.com/vpc/.

[15] P. Murray, A. Sefidcon, R. Steinert, V. Fusenig, J. Carapinha, 2012, "Cloud Networking: An Infrastruture Service Architecture for the Wide Area," IEEE Computer Society,8.

[16] P. Murray, 2011,"D-D.1 Cloud Network Architecture Description," http://www.sail-project.eu/deliverables.

[17] T. Benson, A. Akella, A. Shaikh, S. Sahu, 2011, "CloudNaaS: A Cloud Networking platform for Enterprise Applications," IEEE Computer Society, 13.

[18] B. Luo, W. Liu, 2011,"The Sustainability and Survivability Network Design for Next Generation Cloud Networking," IEEE Computer Society, 6.

[19] B. Ahlgren, P. Aranda, P. Chemouil, S. Oueslati, L. M. Correia, H. Karl, M. Sollner, A. Welin, 2011, "Content, Connectivity, and Cloud: Ingredients for the Network of the Future," IEEE Computer Society, 9.

[20] V. Fusenig, A. Sharma, 2012, "Security Architecture for Cloud Networking," IEEE Computer Society, 5.