Designing Hybrid Cloud Computing Framework using OpenStack for Supporting Multimedia with Security and Privacy

Isaac Cushman
Department of Electrical Engineering
Georgia Southern University
Statesboro, GA USA
lc00214@georgiasouter n.edu

Lei Chen
Department of Information Technology
Georgia Southern University
Statesboro, GA USA
lchen@georgiasouthern .edu

Danda B. Rawat
Department of Electrical Engineering
Georgia Southern University
Statesboro, GA USA
db.rawat@ieee.org

Nhien-An Le-Khac
Centre for Cybersecurity & Cybercrime Investigation
University College Dublin
Dublin 4, Ireland
an.lekhac@ucd.ie

ABSTRACT
Cloud computing is a rapidly growing resource for large data and has spark interest for innovations in the design and security of this new type of big data architecture. One of the major concerns with cloud data storage is that the owners of the information give up the direct control of their information; this leads to significant rise in the need for technology innovations in cyber security. Multimedia applications such as medical images and videos, secure video conferencing, and video streaming consume massive amounts of data requiring significant numbers of servers to provide services for large populations that use them. It becomes increasingly important that the sensitive data offered through cloud resources is to be kept confidential to the respective users without violating confidentiality, integrity and availability of the data. We propose to implement a private cloud which uses a Smart Load Balancer and Bandwidth Shaper (SLBBS) using OpenStack architecture to determine the appropriate action for a user's request in order to better secure data accessed in Multimedia Cloud Networks (MMCN). Our system will allow for privacy sensitive multimedia data to be allocated to specific private cloud computer instead of being sent to public cloud.

Keywords
Cloud Based Network, Private cloud, Smart Load Balancer and Bandwidth Shaper, OpenStack, Hybrid Cloud, Hypervisor, Cloud Controller

1. INTRODUCTION
Cloud network capabilities find strength in the ability to operate as a service – cloud as a service allows users to use its resources dynamically where user demands grow or shrink on-the-fly depending on their operating environment and user demands. Multimedia applications, such as video conferencing, require time sensitive processing in order to maintain a high quality-of-service between any participating parties; in other cases, such as recorded video streaming, we may consider the information to be non-time sensitive due to the fact that the video can be stopped and played multiple times. Cloud based networks operate with the ability to connect to and program virtual operating systems through the means of the Internet. In some applications this can be Virtual Private Networks (VPN), where a user can remotely connect to and operate their personal computer through a cloud based network (CBN). Another application of CBN is the ability to share and write on documents that others are also connected to at the same time.

The information stored in a publicly or privately owned storage may see problems with accessibility or security when many users are able to connect to it. This ideology is supported through the concept of Cloud as a Service, aka. CaaS. This term has three major concepts, Software as a Service, Infrastructure as a Service and Platform as a Service, or SaaS, IaaS and PaaS, respectively. SaaS is able to provide users with application based computing without the need of storing the application on the physical hard disk of their machine [1]; IaaS can provide the user with hardware, software and storage through the Internet [2], and PaaS delivers operating system and application development tools over the Internet [3]. The strength that comes with CaaS is that a combination of each of these concepts can be purchased by the user and provides the ability to run their entire company with little need of large on-site data centers. However in this scenario privacy and security become a very essential asset. There are many different options when creating a CBN, and one of the most widely used is OpenStack. OpenStack [4] has a large community that is constantly using, critiquing and updating how the system operates for many different tasks. Further uses and development of OpenStack is explored later in this paper.

Various proposed solutions to the secure, high traffic demands of cloud computing have already been implemented by companies such as Amazon, who has employed several techniques in cloud service, such as elastic load balancer [5], to maintain availability to their large servers. Microsoft has also created their own cloud service, Microsoft Azure, which provides several different

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264085

services to manage big data and company portfolios managed through their service [6]. Other popular techniques have been applied to allow for portions of a public cloud server to be rented out for private use; however this raises several concerns, such as the loss of availability if the public cloud is hit with a denial of service attack, and the private sector would also be inaccessible. In this paper we explore several techniques that have been used to provide better quality and security to cloud servers in multimedia access and also relate to how a smart load balancer could be employed to make current methods better. In this research we propose a hybrid cloud where the Smart Load Balancer and Bandwidth Shaper (SLBBS) selects the best suited cloud (private or public) based on sensitiveness and delay requirements of the request.

The remainder of this paper is as follows. Section 2 discusses related works that have been used to implement secure cloud networks, section 3 discusses the proposed architecture and model design, section 4 discusses future work for this research, and section 5 concludes the paper with remarks of what this research offers.

2. Related Work

Several topics within cloud infrastructure and research for multimedia data streaming and access have been researched and developed in the attempts to create the best cloud architecture. In this section we present these topics by describing the innovations from the works on the CBN. A common concept that most network developers come across when developing a cloud network is the possibility of a hybrid cloud; that is a cloud which contains both a public and private sector. This structure provides levels of security that are not applicable to a solely public or solely private cloud and brings about the purpose of a smart load balancer for multimedia cloud traffic.

2.1 Multimedia Access in Cloud Computing

In this section, we explore the key attributes that connect multimedia data and cloud computing. The design of an algorithm that can handle multimedia data, data storage and access becomes a trying task. The first design concept that needs to be addressed is how to conform several data types and device communication protocols into a uniform protocol. Next to address is how to securely store and distribute this data to the intended users upon request.

2.1.1 Heterogeneity in Cloud Networks

Multimedia data takes the form of many different types, whether it be photographs, videos, or sound clips. Along with them are several types of devices with varying security and communication protocols in which they connect to the Internet. This issues cause a concern for data analysts and developers with security in mind. It is important to build a cloud structure that can handle various data types and has the ability to serve the many types of devices connected to the network. The research in [7] proposes one such method to handling heterogeneity in networks with the IP Multimedia Subsystem (IMS) framework. The IMS framework uses the three concepts of as-a-service mentioned earlier in order to build a mechanism that is capable to maintain high quality of service, QoS, manage computing services and user preferences and allows for users to access specific applications in the cloud with IaaS, PaaS and SaaS, respectively.

2.1.2 Multimedia Distributed Data Storage

As addressed previously, a major challenge in the storage of a cloud network that provides user media access is the ability to adapt to the specific user's media request, communication protocols and the actual system requirement that particular type of media requires. It would also require the overall cloud network to pull data where the network may exist virtually in very different locations, increasing the cost of transmission of data. It is possible in a cloud network to provide methods for specific types of data to either be placed in or converted to appropriate data type tables in order for the computing system to categorize a user request to maximize efficiency. This ideology is explored in [8] with the use of applying a virtual service model (VSM) hierarchy. In this method they design the system to contain a root layer, containing all possible data that could be requested through the cloud. Then a new layer is introduced for each general type of media. High resolution requests from users will take a higher precedence in the hierarchy compared to low resolution media types. Also mentioned in the work is the problem with redundancy in the layers because each new layer is constructed on the basis of the root; it does however bring to surface a possible way to distribute data for storage inside a cloud.

2.1.3 Confidentiality, Integrity and Accessibility

Security schemes in data storage offer certain levels of confidentiality, integrity and accessibility to a network system; for example a specific scheme may require the user and provider to share a service level agreement (SLA) which will continually check if what is being stored is agreed upon by both parties. In cloud computing, this system is more complex and has many areas where potential malicious users would be able to steal, change or destroy valuable data. In this section, the framework proposed in [9] is explored in order to generate better data integrity and confidentiality for our multimedia cloud network. For data integrity, the proposed method uses two concepts: a Third Party Auditor (TPA) and Proofs of Retrievability (PoR).

TPA is a mechanism used to gain trust between the service provider and the user in the network. This mechanism is built by monitoring the data stored in the cloud and its interaction with the cloud provider. A homomorphic authenticator is used to audit the data sent by the data owner and generate a corresponding result. A potential draw back in this system is the possibility of revealing the data owner's identity if a malicious user was to sniff the data audit. This could be fixed, however, by using data masking techniques and encryption schemes. Figure 1 below demonstrates the typical design of a TPA system.

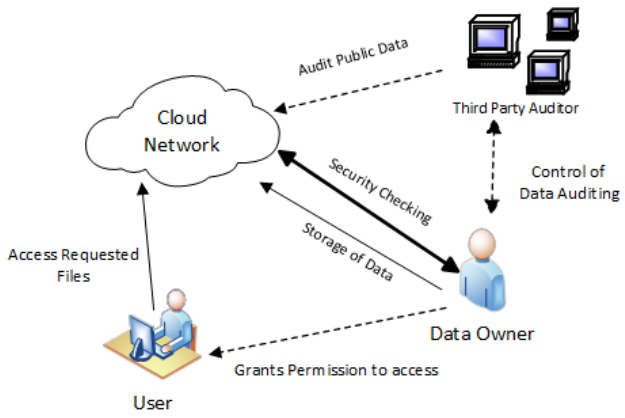

Figure 1. Third Party Auditor Topology.

For obvious reasons it is critically essential to keep multimedia data, either being streamed from a video conference or stored from medical procedures, confidential to only the users with the proper authentication. Several proposed works mentioned in [9] cover different schemes to provide confidentiality in cloud networks. One method is the use of cryptographic algorithms placed on the data blocks with the key given to the data owners. This ensures that the data stored in the cloud can only be accessed by data owner. Another method is the use of secure provenance model, recording the ownership and the process history to increase the trust of the data owner to the network. Additionally, the use of a fully homomorphic encryption (FHE), was proposed by Craig Gentry. This encryption technique allows circuit evaluation over encrypted data without being able to decrypt it, allowing for better confidentiality. However it may restrict the distribution of data for the data owner trying to access from multiple locations.

2.2 Hybrid Cloud

In this section, we explore a concept that may better distribute chunks of data based on type, security requirement, or traffic volume. The idea of renting out small sectors of a cloud to paying subscribers is a viable concept to cloud service providers. This allows them to allocate portions of their network that may not have been fully utilized. Having a public and private cloud exist inside the same overall structure provides significant increases to usability. However it comes with new types of security risks to consider. The research work in [10] considers the effects of placing a cloud inside the cloud, otherwise known as a hybrid cloud. Demonstrated in Figure 2, this model allows for a small subsection of the public cloud to be exclusively owned by an administrator while still keeping data links to other parts of the public cloud. The private cloud is able to act as both its own structure and still remains connected to either the entire public cloud or via certain specific data links, depending on the need and configuration of the private cloud. In this model, it is possible to reduce the cost of communication between public and private than traditional sense of hybrid cloud where the two clouds act as separate entities.

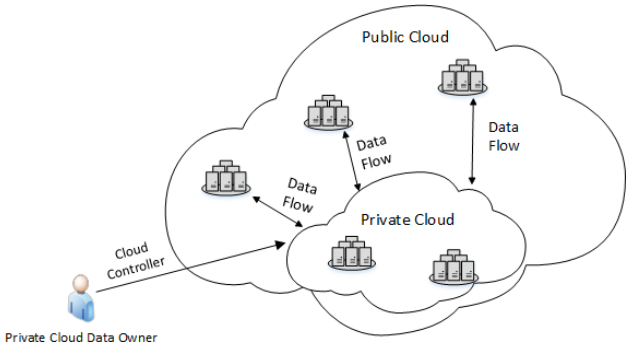

Figure 2. Cloud in Cloud Model.

The cloud-inside-cloud configuration brings around a new ideology on how to manage private sectors in cloud based networks. However it does not consider the effects on heavy multimedia traffic access that would occur when many private networks call on a public cloud at the same time. In this scenario, we consider innovating onto the cloud in cloud structure, by applying methods found in private cloud frameworks to achieve the goal of creating a load balancer that will distribute data quickly amongst large cloud networks.

2.3 Private Cloud Infrastructure

One of the main challenges when managing a cloud network for users to store and access data is the ability to maintain confidentiality, availability and integrity of the system. One of the key problems comes from the need of a uniform security intrusion and detection method to be employed over the cloud. A cloud network could not allow for individual users to access and change security parameters simply because otherwise the availability to sectors of the network would break. The research in [11] establishes several concepts of private cloud security. First they introduce a private virtual infrastructure (PVI), where the data owner and cloud operator are in common terms of security protocol while the virtual datacenter stays in direct control of the data owner. In this scenario, it is obvious that role based interactions will control the structure of the cloud where both the operator and the client would need to establish service level agreements before establishing a secure connection. The concept of Trusted Platform Module (TPM) is also introduced in their research. This module stores cryptographic keys in the platform configuration registers (PCRs) and establish the access of the clients to their configured platform. Based on this architecture, a certain level of trust is formed in the cloud network as only specific users will be able to access specific sections of the network. This concept builds a two layer architecture for private cloud security, the IaaS fabric layer and the PVI layer, establishing important rule based operations for both vendor and data owner.

2.4 Cloud and Virtualization Technologies

OpenStack provides an IaaS for users to develop cloud networks. It uses several components in order to design their cloud computing architecture, consisting of the essential blocks: the cloud controller, compute node, network node and optional storage node [12]. Figure 3 demonstrates the typical architecture of an OpenStack private cloud service [12].

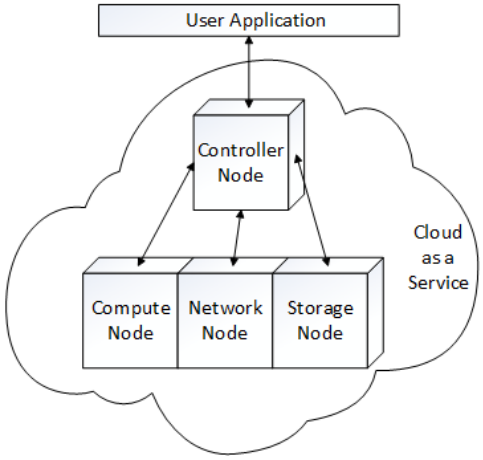

Figure 3. Cloud Network Using OpenStack based Topology.

The controller runs the virtual machine Identity and Image services, management portion of compute node and the dashboard. The dashboard is a web-based interface that users can use to interact with OpenStack services, such as launching an instance and assigning IP addresses. It also serves as a means for the data owner to interact with their data, through queries, entry tracking and utilization of their cloud server. The controller node is also capable to operate as a storage block and cloud operator, generally used to access the network and compute node in order

to run the cloud server. The compute node is responsible for the hypervisor that operates tenant virtual machines or instances, connects network plug-ins and firewall services. It can also contain a third network interface in the storage to improve system performance. The network node runs the networking plug-in and several agents to provide switching, routing, Network Address Translation (NAT) and Dynamic Host Control Protocol (DHCP). A list of the core services in OpenStack is given in Table 1. These services each have a project name inside OpenStack, which may cause confusion to users configuring the network for the first time. To avoid such confusion, the core services and their counterparts are listed in pairs (in the same row) in Table 1. This information and the discussions in the following section are useful in helping us determine the appropriate structure, model, system, operating system, software and hardware for building our own private cloud in this research.

Table 1. Common OpenStack Services and their corresponding Related Project Name

Core Services	Project Name
Dashboard	Horizon
Compute	Neutron
Object Storage	Swift
Block Storage	Cinder
Identity	Keystone
Image Service	Glance

2.4.1 Choosing OpenStack based on Comparisons

Many works have tried to compile reasoning as to which set of technologies and software can provide the best solution to the needs for cloud and virtualization. The current problem exists that there is no one best solution as each has its own strengths and weakness, and finding the best solution for a specific scenario truly depends on many factors, such as the research goals and scope, network scale, available funding, as well as technical support (i.e. IT service involvement). Research in [13] and [14] provides comparisons about the important features of Hypervisors and cloud computing technologies, which serves as a guide when selecting specific operating systems.

For the purpose of building the private cloud for our future research, we first consider features that exist in VMware compared to OpenStack, as shown in Table 2. One of the most beneficial facts about OpenStack is that it is an Open-Source software that does not require the purchase of a license. Also OpenStack is able to run mostly on its own platform, such as Horizon, Nova, and Cinder, which have been designed specifically for use of cloud networks, whereas VMware uses certain technologies not specifically designed for its software. While this may not always pose a problem, it is considered to be safer choosing OpenStack to avoid configuration and coding problems when building our network server.

Table 2. Comparison of Features of VMWare and OpenStack Virtualization [13]

Feature	VMware	OpenStack
Hypervisor	Type 1 virtualization, ESXi	Type 2 virtualization, e.g. KVM, ESXi, Hyper-v, Xen, Baremetal
Customer Access	Windows Client, Web console, API	Open API, Command Line, Horizon (Dashboard)
Network	Switching network, NSX for SDN	Switching, pluggable extensions to SDN like OVS
Storage	SAN, iSCSI	Pluggable Cinder
Image Management	Catalogs, VM templates and OVF, upload iso to Data store	Glance image service, custom flavors and images can be created
Costs	Licensed	Free/Open-Source
Management System	vCenter cannot distribute its services	Nova-Controller can distribute its services
Scheduler	DRS with load balancing features, manages workload 'intelligently' by grouping virtual machines, pooling resources of physical hosts and prioritizing VMs in these pools.	Nova-Scheduler, does not support DRS features but can be implemented using external monitoring, Filter Scheduler and Live Migration

Following the above comparison, we explore options for the hypervisor. This part of the network is important due to the fact that the hypervisor is responsible for running each instance of the Virtual Machines in the network. Based on information in Table 1, it is known that OpenStack can use KVM, HyperV, and Xen hypervisor. Table 2 compares them for an overall efficient solution. One of the stand out benefits, according to [14], to using KVM over Xen or HyperV is the ability for guest users on the network to be able to have any desired operating system, which greatly diversifies the traffic population allowed in the network. HyperV has strengths in that many popular OS can be used in it, it can run both 32 and 64 bit versions, and it opens shareware to use. If licensing cost is not an issue, HyperV may also be a good option to consider.

Table 3. Comparison of Select Hypervisor Technologies [14]

	Xen	KVM	HyperV (Microsoft)
Host OS	Linux (certain versions)	Linux	Win 7, vista, XP; SUSE Enterprise Linux, Redhat Enterprise Linux
Guest OS	all Windows and Linux versions, Solaris	all	Win 7, vista, XP; SUSE Enterprise Linux, Redhat Enterprise Linux
Type of	Para-Virtualized, Full-Virtualized	Full-	Para-Virtualized

Virtual.	and AMD-V Technologies	Virtual.	
Platform	x86, x64, PowerAMC and ARM	x86	x86, and x64
Virtual. Enabled	with / without	with	with
Live Migration	Yes	Yes	only with Cluster Shared Volumes
Cloud Uses	Amazon, Cloud.com and Rackspace		
Free / Shareware	GPL License	GPL License	Shareware

The last comparison from the work presented in [14] is among specific cloud computing technologies, specifically Eucalyptus, Xen Cloud platform and OpenStack. Each of the technologies offers a wide range of options, including operating systems. The key advantage of using OpenStack is the architecture and programming supported with a large data supply of documents and key concepts on how to use this software. A limiting factor however, is that the current version cannot run on 64 bit systems whereas the other systems are more versatile.

Table 4. Comparison of Cloud Computing Technologies [14]

	Eucalyptus	**Xen Cloud Platform**	**OpenStack**
Main Purpose	EC2 Cloud	Evolution of Citrix XenServer	Offers Cloud Computing Services
Users	Enterprise	Enterprise	Enterprise, service providers, and researchers
Supported OS	Linux (Ubuntu, Redhat Enterprise Linux, Fedora et SUSE Linux Enterprise Server)	Linux (Fedora, Redhat, CentOS et SUSE Linux Enterprise Server) and Windows 7	Linux, Windows and requires x86 server
Architecture	Hierarchal, five components, and a minimum of two servers	Centralized, three components and a minimum of two servers	Integration of OpenStack object and OpenStack compute
Language	Java, C and Python	Caml	Python
Storage	SCP and SQLite3	VastSky	OpenStack Store
Network	DHCP Server on the cluster	Open vSwitch	OpenStack
	controller		Compute
Access Interface	EC2 WS API, Tools as: HybridFox, ElasticFox	Command Lines XE (XenCenter and Versiera (commercial solution for windows)	Web interface
Load Balancing	Cloud Controller	XAPI	Cloud Controller
Fault Tolerance	Cluster Controller's separation	Virtual Machine state synchronizer	Replication
Live Migration	-	Open Virtualization format, shared storage	-
VMs Location	Node Controller	XCP Host	OpenStack Compute

3. Proposed Architecture and Model

Our proposed model presents a new algorithm that will take a user's request and generate a response based on authenticity, trust level and multimedia data type, and correspondingly grant access to the stored data. In the event that the data is open to the public, such as video streaming applications, the algorithm will call the appropriate portion of the cloud network where data is stored as not to disrupt any current data being streamed from a cloud portion with private or higher security level. Figure 4 depicts the proposed model, where a private cloud network for Georgia Southern University contains secure (multimedia) data for official use by faculty, which is kept separate from the network where public data, such as information about sports events or academic news, is accessible by all. An algorithm to be built inside the SLBBS will serve as pathway for all user requests that wish to have access on the cloud and direct the request to the appropriate network.

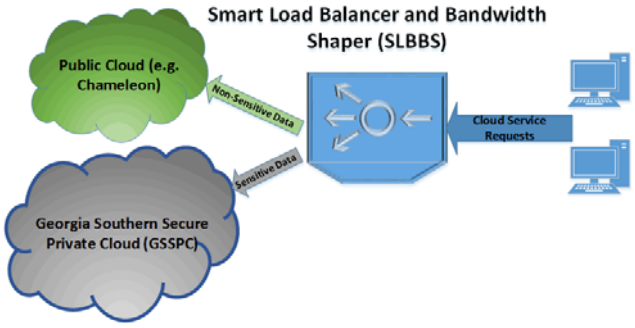

Figure 4. Proposed Infrastructure includes a Smart Load Balancer and Bandwidth Shaper (SLBBS) and Georgia Southern Secure Private Cloud.

Based on the above studies in this research project, the hardware of the proposed infrastructure requires a minimum of three rack servers: a controller node, a network node, and a compute node.

The controller node runs the virtual machine Identity and Image services, management portion of Compute, and the dashboard. This server provides service to both Georgia Southern Security Private Cloud (GSSPC) and SLBBS. The network node runs the networking plug-in and several agents that provision tenant networks and provides switching, routing, Network Address Translation (NAT), and Dynamic Host Configuration Protocol (DHCP) services. This rack server will be configured and modified to function as the SLBBS. The compute node runs the hypervisor that operates tenant virtual machines or instances, using Kernel-based Virtual Machine (KVM) as the hypervisor. The compute node also runs the networking plug-in and an agent that connects tenant networks to instances and provide firewall (security groups) services.

The software of the proposed infrastructure, including Red Hat Linux, OpenStack with KVM (Kernel-based Virtual Machine) and Linux-based open source software and tools are free of cost. OpenStack with KVM solution is one of the most popular open source cloud operating options with excellent scalability. In addition to the embedded security features provided by OpenStack, Linux based open source security and forensic software and tools, such as Snort IDS/IPS, The Sleuth Kit (TSK), and RainbowCrack, are all available free of cost. These combined advantages provide great potential for future collaborative research in multimedia networking and cloud security and digital forensics with the flexibility of growth in scale.

4. Future Work

Innovating the ideas explored in this paper and the comparisons made with current technologies, the goal of this research project is to support current cloud technologies with better security algorithms and provide a better means for users to store and access their sensitive multimedia data. With further research, we will implement this concept with a three tier rack sever system consisting of a controller, compute and network nodes. The designed network will then allow the deployment on a small, controlled scale which forms a test bed for this system to potentially grow into a fully realized and deployable cloud network for future research on highly time sensitive video, imaging and other multimedia communication and applications.

5. Conclusion

Data security over the cloud/Internet is an essential part of sharing multimedia access to insure that confidential information is not stolen, distributed or destroyed. In this paper we have first presented current status and challenges in technology design and innovation in multimedia data access and storage in cloud networks. We then presented the existing cloud technologies and provided a comparison for potentially the most appropriate solution for implantation. We also presented a new framework to for providing security to multimedia access in the cloud with a smart load balancer and bandwidth shaper. To conclude we presented the possibilities for further applications for the proposed framework and how it will further benefit cloud computing networks and technology innovations as a whole.

6. ACKNOWLEDGMENTS

This research has been funded by the Georgia Southern University College of Engineering and Information Technology (CEIT) Faculty Research Seed Grant.

7. References

[1] Kulkarni, G., Mandhare, S., and Bendale, D. 2012. Software as Service Cloud. *2012 International Conference on Computer Science and Service System.* (2012).

[2] Dawoud, W., Takouna, I., and Meinel, C. 2010. Infrastructure as a service security: Challenges and solutions. *Informatics and Systems (INFOS), 2010 The 7th International Conference on.* (2010), 1-8.

[3] Krebs, R., Loesch, M., and Kounev, S. 2014. Platform-as-a-Service Architecture for Performance Isolated Multi-tenant Applications. *2014 IEEE 7th International Conference on Cloud Computing*. (2014).

[4] "Software » OpenStack Open Source Cloud Computing Software", OpenStack.org, 2016. [Online]. Available: https://www.OpenStack.org/software/.

[5] "Elastic Load Balancing", Amazon AWS, 2016. [Online]. Available: https://aws.amazon.com/elasticloadbalancing/.

[6] "What is Azure—the Best Cloud Service from Microsoft | Microsoft Azure". Microsoft, 2016. [Online]. Available: https://azure.microsoft.com/en-us/overview/what-is-azure/.

[7] Chen, J., Wuy, S.,Larosa, Y., Yang, P. and Li, Y. IMS cloud computing architecture for high-quality multimedia applications, *2011 7th International Wireless Communications and Mobile Computing Conference*. (2011).

[8] Korotich, E. and Samaan, N. A novel architecture for efficient management of multimedia-service clouds. *2011 IEEE GLOBECOM Workshops (GC Wkshps).* (2011).

[9] Huang, C., Qin, Z. and Kuo, C. Multimedia storage security in cloud computing: An overview. *2011 IEEE 13th International Workshop on Multimedia Signal Processing*. (2011).

[10] Zhang, H., Ye, L., Du, X., and Guizani, M. Protecting private cloud located within public cloud. *2013 IEEE Global Communications Conference (GLOBECOM)*. (2013).

[11] Krautheim, F. Private virtual infrastructure for cloud computing. *Proceedings of the 2009 conference on Hot topics in cloud computing.* (2009).

[12] "Chapter 1. Architecture - OpenStack Installation Guide for Ubuntu 14.04- juno", Docs.OpenStack.org, 2016. [Online]. Available: http://docs.OpenStack.org/juno/installguide/install/apt/content/ch_overview.html.

[13] Sahasrabudhe, S. and Sonawani, S. Comparing OpenStack and VMware. *2014 International Conference on Advances in Electronics Computers and Communications*. (2014).

[14] Mahjoub, M. Mdhaffar, A., Halima, R. and Jmaiel, M. A Comparative Study of the Current Cloud Computing Technologies and Offers. *2011 First International Symposium on Network Cloud Computing and Applications*. (2011).