

## Cloud Computing: 360 Degree Reference

Mona A. M. Fouad<sup>1</sup> and Ahmed Mokhtar A. Mansour<sup>2</sup>

<sup>1</sup>*Computers & Systems Department*

*National Telecommunication Institute, Cairo, Egypt*

<sup>2</sup>*Nile Innovations, Cairo, Egypt*

<sup>1</sup>*mfouad@nti.sci.eg,* <sup>2</sup>*ahmedmokhtar\_adu@yahoo.com*

### **Abstract**

*This paper presents a full image about Cloud computing by describing in details the Cloud computing components, the deployment framework, Cloud services, and Cloud contributors, reviewing the standardization efforts and research challenges as well as the current and future opportunities for investment. The full image is accomplished by demonstrating our experimental experience for deploying the Cloud computing environment based on OpenStack. Furthermore, this work reviews the literature for the most recent research work considering service management, Virtual Machine migration, load balancing, Green Cloud, privacy and security. The study shows that a lot of work is still needed to provide services that are available, reliable, and secured with minimum cost, maintaining power saving and best utilization of resources. Coinciding with developing services efficiently, the huge amount of data that Cloud computing deals with extends the work in the Internet of Things, and Big Data.*

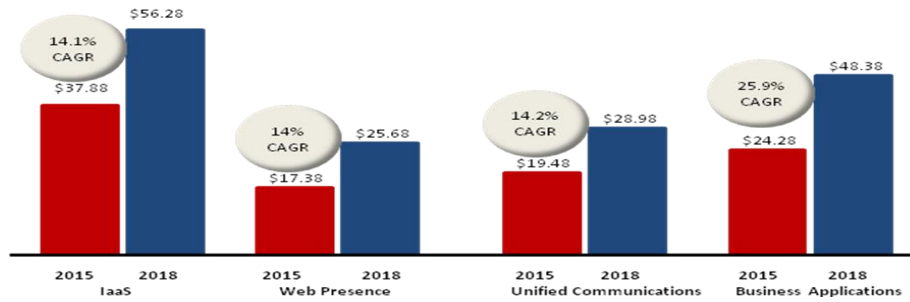
**Keywords:** *Cloud Computing, Load balancing, OpenStack, service composition and provisioning, Green Cloud, security and privacy, VM migration*

### **1. Introduction**

Cloud computing began as a web hosting service, and then evolved continuously to provide hosting for data, applications, and processing as well. It has several advantages over the traditional data centers, such as mobility, cost reduction, collaboration, *etc.* On the other hand, there are several challenges; namely, privacy and security, reliability and availability, performance concerning bandwidth cost, *etc.* The benefits versus challenges recall the need for a comprehensive study that encompass all around the Cloud computing environment as a whole.

The Cloud computing is developed through several milestones. The era of Cloud computing began when John McCarthy of US Advanced Research Projects Agency (ARPA) stated the ability to provide and organize the computation as a “utility”, providing the first version of the Internet in 1970. In the same time, IBM developed the virtual machines (VMs) in early 70’s of the previous century. The built of the first web server by Tim Berners-Lee in 1989 is another important milestone. After that, Salesforce in 1999 and then Amazon Web Service (AWS) in 2002 lunched the concept of delivering enterprise applications via website to provide simple web service hosting. By announcing the Amazon Elastic Compute Cloud (EC2) in 2006 and the deployment of Google APPS in 2009, the Cloud computing services started. Two platforms are then developed in 2010; namely Azure by Microsoft and the open source ‘OpenStack’ by NASA and Rackspace.

According to Gartner report, the migration from traditional to Cloud computing is one of the top priorities on the agenda of enterprises Chief Information Officers (CIOs). The distribution of workloads between traditional data centers and Cloud based data centers evolved from 70%-30%, respectively in 2011, to around fifty-fifty in 2014, and then pictured to be 38%-62%, *i.e.*; about 50% market-share reduction since 2011.



**Figure 1. Market Investment Forecast through 2018 (Odin)**

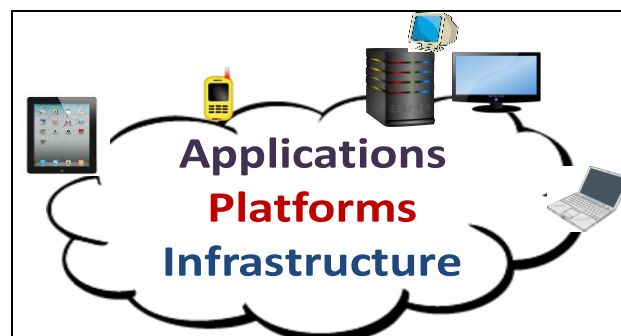
Odin market research firm released a business analysis report in 2015, stated that the SMB current investment is 99 billion USD and it will reach around 160 billion USD in 2018. As shown in Figure 1, the Compound Annual Growth Rate (CAGR) is about 26% for SaaS, and 14% of IaaS and PaaS (web and unified communications), respectively.

The demonstrated historical background and the existing market share explored the importance of Cloud computing as the current and far future of computing. The rest of this paper completed the overall picture of Cloud computing as a utility. The Cloud computing environment is described in Section 2. The existing proposed cloud architecture models are reviewed in Section 3. The standardizations efforts and the existing cloud platforms are demonstrated in Sections 4 and 5, respectively. The challenges and the most recent research review is presented in Section 6. Finally, Sections 7 and 8 comprise experimental experience of establishing the Cloud computing environment based on OpenStack and the conclusion of the proposed work, respectively.

## 2. Cloud Computing Environment

Cloud computing is defined as a model for sharing a pool of configurable computing resources through the Internet. As shown in Figure 2. Cloud computing environment contains the hardware infrastructure, the platform to deploy the environment model, and the services to be provided. All these components are explored in a layered architecture.

Carrier, broker, auditor, provider, and consumer are the main actors of this environment. The two main stakeholders are the provider and the consumer. However, to have a sustainable scalable model, the existence of the other actors is essential. The Cloud carriers perform mainly the communication part of the Cloud scenarios. The Cloud broker provides service intermediation, service aggregation, and service arbitrage. The Cloud auditor is a third party that performs review and insurance activities over other Cloud actors. The Cloud provider performs five major tasks, namely; service deployment, management, orchestration, security, and privacy. The Cloud consumer is any entity that uses the Cloud services from a provider [1].



**Figure 2. The Cloud Computing Environment**

## 2.1. The Deployment Model

A deployment model differentiated from another by the access scope of the Cloud environment. The three models adapted by all organizations working on standardization are private, public, and community. In private model, the owner organization installs and manages the physical infrastructure under full control of all layers. In Public model, services are provisioning from anywhere. Such access might be free or payable. The Cloud is dedicated to a specific community for a specific purpose in the community model. Different stakeholders who have interest in such a purpose will share the resources of the community Cloud. Purpose could be business oriented, technology oriented, or/and security oriented, *etc.* One or more stakeholders of the community, a third party, or a consortium of them might own the Cloud, concerning the management and ownership part.

## 2.2. The Service Models

The major well-established service models are Software as a Service (SaaS), Platform as a service (PaaS), and Infrastructure as a Service (IaaS). During the booming of Cloud computing concept, many technical and marketing documents proposed other service concepts. To avoid the jungle of acronyms produced by the environment (NaaS, CaaS, TaaS, *etc.*), a new term was introduced as XaaS, which means “anything as a service”.

In SaaS, the application is running on the provider premises but the user has full access to use this application. ‘Google Apps’, Customer Relationship Management (CRM) by SalesForce, ‘Zoho’ as a large suite of web-based applications for enterprises use mainly, and the Microsoft Office 365, are some examples for SaaS service model.

PaaS covers servers hosting, security, CMS, CDN, and other communication supporting tools. The consumer may deploy and manage his own application over the providers’ platforms. Google App Engine platform to develop and run Java, Python, and Go applications on Google’s infrastructure and Microsoft Windows Azure to compute, store, and deploy platforms for Windows applications, are two well-known PaaS examples.

In IaaS, consumers have full control over the virtual infrastructure that includes VMs, networks, and operating systems over virtual machines, *etc.* The most common examples for IaaS services are Amazon EC2 and S3. Amazon Elastic Compute Cloud (EC2) provides special virtual machines, called Amazon Machine Images (AMI) that deploy and run over the EC2 infrastructure. Amazon Simple Storage Solution (S3) provides dynamical and scalable storage resources.

## 2.3. Virtualization

Despite of the hardware capabilities that providers could afford, the numerous amounts of tasks to be performed are millions of times greater than the available resources. This invokes virtualization to take place. The concept of virtualization is an old concept; however, the evolution of virtualization is one of the leading forces in Cloud computing technology widespread adoption. Virtualization started in the 70s of the 20<sup>th</sup> century when IBM introduced the VM concept. The word virtual machine became very popular in 90s when the java internal virtual machine concept for code portability.

Virtualization means “the ability to run multiple operating systems simultaneously on a single physical system, sharing the underlying hardware resources”. This is done through running several virtual machines over the same physical system. In order to allocate and manage the sharing of resources between the virtual machines and the physical systems, a virtualization manager (hypervisor) should be deployed.

The virtual environment has two types, hosted and bare-metal. For the hosted virtualization, the underlying physical hardware has its own operating system. In this case, the hypervisor is seen as a layer of interface between the virtual machines and the

native operating system installed over the physical hardware. The hypervisor maps the virtual machine requests to the native OS instruction set to perform the resource sharing. For the bar-metal virtualization, the hypervisor deploys its own kernel to boot and manage the physical hardware resources.

## 2.4. Cloud Service Management

The Cloud service management interacts with the software, abstraction (virtualization and platforms), and physical layers in order to provide business support, provisioning/configuration, and portability/interoperability.

From functional point of view, there exist two types of service managements. The first interacts directly with the computing layers (IaaS, PaaS, and SaaS). The second is the inter-service management that deals with the Cloud control and administration such as interaction with different actors, conducting the necessary monitoring, security and privacy services.

The inter-service administration composes of three main tasks. The first is the business support that includes the consumer management, contract management, inventory management, reporting and auditing, accounting and billing, and the pricing and rating services. The second major task is the provisioning/configuration, including service provisioning, resource allocation, monitoring, reporting, metering, and SLA management. The third major task of the Cloud service management is the portability/interoperability, which includes data portability, data copying, bulk data transfer, service interoperability, unified management interface, system portability, VM image migration, and application/service migration.

## 3. Cloud Computing Architecture

The maintained characteristics distinguish among Cloud computing service models, while the Cloud computing architecture maintains the framework (architecture) for providing its services with specified characteristics. The general Cloud computing architecture provides the three layers of the service model.

Cloud computing Open Architecture (CCOA) is suggested in [2]. It supports the Cloud computing architecture by integrating the management of resources and services in a unified Ecosystem that provides three dashboards for Cloud vendors, brokers, and users as well as the unified information exchange framework, as shown in Figure 3.

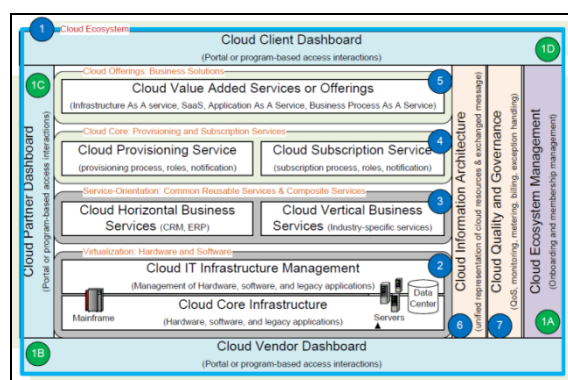


Figure 3. The Cloud Computing OPEN Architecture [2]

A service-oriented architecture is proposed for interoperability among different Clouds in [3]. The architecture is composed of four layers; namely, the hardware and infrastructure layer, the virtualization layer, the ontology layer, and the service

management layer. The service management includes application load balancer as well as the service load balancer.

Reference Architecture (RA) for Cloud-based Tools as a service workSPACE (TSPACE) is presented in [4]. The platform is designed for provisioning chain of tools following the Software as a Service (SaaS) model with three levels of abstractions for service management, namely; information gathering and awareness, semantic integration and finally the service provisioning level.

Generally, any Cloud computing architecture is composed of two parts, the front-end and the back-end. The front-end concerns about the visible part of the Cloud architecture encountered through web-enabled devices. The back-end comprises all resources required to deliver the Cloud computing services, such as virtual machines, security mechanisms, storage facilities, *etc.*

#### **4. Standardization Efforts**

The worldwide use of Cloud computing requires unification of frameworks and functionality of the delivered services. Several efforts are going on to globalize the use of Cloud computing while maintaining sufficient quality of services provided. According to ITU perspective, there exist six major standardization areas [5]. 1) Rich access for users and partners, covering user access over communication media using different types of devices from different locations. 2) Interoperability between Cloud providers, covering methods of communication and exchanging data in a full transparent and automatic manner with the ability to easily move workloads and data from one Cloud provider to another or between different Clouds. 3) Modular Cloud functional architecture, compromising everything as a service or XaaS trend to be responsive to the new needs. 4) Security and privacy, covering authentication, authorization and encryption of data in order to protect both the computing environment and the personal information. 5) Elastic network and infrastructure, to be able to provision and release of resources automatically in an effective and rapid manner. 6) Cloud management that covers all the tasks in the Cloud management layer.

The year 2012, witnesses many efforts in Cloud management standardization efforts. Open Grid Forum (OGF) and Distributed Management Task Force (DMTF) are active on the standardization of APIs for managing Cloud resources. Storage Network Industry Association (SNIA) is active of standardization of APIs for Cloud storage. Global Inter-Cloud Technology Forum (GICTF) covers the domain of inter-Cloud interoperability standards. TeleManagement Forum (TM Forum) performs standardization efforts for Cloud service management. OASIS carries out the standardization for identity services in the Cloud, while the Cloud Security Alliance addresses the security aspects. Activities in ISO, ITU-T, and NIST are addressing the standardization of Cloud definition, architecture, and ecosystem. The IETF and W3C are active on access and protocols aspects. IEEE standardization efforts address the portability and interoperability between Clouds. Two main documents explain the advances in the standardization effort in IEEE, namely; P2301 and P2302 (<https://standards.ieee.org/develop/project/>).

#### **5. Cloud Computing Platforms**

Cloud computing environment is composed of mandatory and optional parts. The first part is composed of platform and few of the management services, while the other is optional such as the advanced management services and Cloud simulators. The mandatory service managements concern about service provisioning/releasing, and monitoring. The advanced service managements concern about the testing, evaluation, and reporting.

Several Cloud computing platforms currently exist, such as OpenStack, Eucalyptus, RedHat's Cloud, Traffic Server, Cloudera, Puppet, Enomaly, Joyent, Zoho, Reservoir,

OpenNebula, AbiCloud, NimBus, Heruko, Amazon Elastic Beanstalk, Windows Azure [6].

## 6. Research: Challenges and Review

Cloud computing challenges comprise portability, availability, interoperability, security and privacy. These challenges are dealt with several efforts in the field of service composition, VM migration, load balancing, green Cloud (energy saving), data privacy and Cloud security.

### 6.1. Service Composition and Provisioning

Service provisioning is the allocation of resources according to customer needs and SLA, maintaining QoS and utilization of resources that may be composed of a set of tiny services.

In [7], a hybrid provisioning system is proposed based on overall load and resource unpredictability, combining the reserved and the on-demand strategies, achieving better performance of applying each individually. VM multiplexing approach is proposed in [8], to save capacity when the peaks and troughs in multiple VMs are temporally unaligned.

Service provisioning is modeled as a Nash game equilibrium problem in [9] to develop a distributed algorithm for run-time of IaaS resources among different providers, concerning QoS and SLA. In [10], provisioning of applications, via SaaS providers, is conducted based on the Stackelberg game, concerning the equilibrium of QoS and maximization of revenue.

Dynamic selection and composition of services from the service pool are surveyed and investigated in [11], addressing composition restrictions, quality of service parameters, and rapid changes in the properties of the services and network, announcing that the classic and graph-based approach is widely used, while the machine-learning and structures are the least used approaches.

### 6.2. VM Migration and Server Consolidation

Virtual machine migration (server consolidation) is the transfer of a virtual machine from one physical machine to another. VM migration is needed for load balancing, energy saving, and during maintenance. The challenge is to transfer the whole content of virtual machine and start task execution on the destination virtual machine promptly. The VM is composed of three components: 1) the connected devices and the internal CPU states (few kilobytes), 2) the local storage devices content, 3) the Random Access Memory content (up to several gigabytes).

The existing VM migration algorithms are grouped into two approaches; the iterative post-copy and the iterative pre-copy. In the iterative post-copy, VM is stopped at source PM and transferred to destination host with its minimal processing state to start its primary execution. In the iterative pre-copy (Live Migration), the contents of the VM's image are first sent to the target host and then the VM is restarted.

In [12], useful pages are identified first, and then compressed them to efficiently decrease the total transferred data, total migration time and downtime. The performance of VM migration is examined for KVM, XenServer, VMware, and Hyper-V virtualization systems in [13], concluding that KVM is outperform others concerning memory migration and storage migration. A careful selection of the proper moment to start migration is important to reduce the live migration penalties. The work in [14] proposed a method to decide whether to start the live migration or postpone it based on the identification of the VM workload cycle, reducing both network data transfer and live migration time.

### 6.3. Load Balancing

Load balancing is the provisioning, placement, and migration of Virtual Machines for the purpose of distributing workloads among active servers. Load balancing approaches are classified as static or dynamic. In the static approach, tasks are assigned to the available VM based on prior information; such as fixed time interval and execution time. In dynamic approach, tasks are assigned to the VM based on information that is collected dynamically.

The dynamic method is performed on two levels; 1) determining of the over/under-loaded resources, 2) taking a decision to apply provisioning, placement, or migration. Honeybee, genetic-based and agent-based algorithms are dynamic load balancing methods that dynamically determine the best VM to receive the current workload.

A comparison among several dynamic algorithms, concerning throughput, response time, fault-tolerance, scalability, performance, and resource utilization parameters is provided in [15].

Geographical distribution, available storage, and complexity of algorithm for collecting dynamic information are the challenges demonstrated for load balancing in [16]. A multi-objective load balancing is found in [17], optimizing the virtual machine placement that minimizes power consumption, resource waste, server unevenness, inter-VM traffic, storage traffic, and migration time, all at the same time.

### 6.4. Green Cloud

Efficient arrangement of physical and virtual resources affect positively on environment. This is explored in two directions; hardware level and software level. The hardware level approach involve slowing down CPU clock, powering off parts of the CPU chips, turn power off of released Physical Machine (PM) after VM migration, *etc.* The software level imply the energy aware task scheduling, by which power consumption of a processor is reduced during task execution. Based on the fact that servers are introduced as the most energy consumer in data centers, both hardware and software based techniques target the data center servers. An intensive study of energy consumption techniques by data center servers and networks in Cloud computing is found in [18]-[20].

The most efficient energy saving techniques for servers include Server Virtualization, Dynamic Power Management (DPM), and dynamic Voltage/Frequency scaling (DVFS) [18]. With respect to the existed solutions for saving energy in data center networks, the Adaptive Link Rate (ALR), Virtual Network Embedding (VNE), Sleep mode, and Green routing is comprised. A solution for improving energy efficiency in data centers is suggested in [19] as well. The solution comprises three-complementary steps; the dynamic resource allocation, the thermal-aware load balancing, and the server consolidation concerning the overall energy consumption. Exhaustive analysis for energy consumption algorithms is presented in [20].

### 6.5. Data Privacy and Cloud Security

Data stored in public should be maintained apart from any tampering, unauthorized access, or getting lost. Several recommendations are mentioned in the literature considering careful selection of the Cloud Service Providers (CSPs), maintaining confidentiality via authentication, authorization, availability of data through regular back-up and recovery, secure the migration process using fingerprint technique for the virtual operation system (VOS), use of secured data transmission by using secured channels, secured browser (HTTPS), IPSec, *etc.* and the use of hardware and software firewalls [21]-[25].

A model for simultaneous data integrity verification and privacy preserving is proposed in [21]. A multi-aspect, memory exclusive approach for precise and robust guest OS fingerprinting in the Cloud is introduced in [22]. A code hash based approach from kernel

code aspect is used to determine the guest OS version. If the code hash approach failed, a kernel data signature based approach from kernel data aspect will be used to determine the OS version. Security of hypervisors are surveyed in [23], focusing on attacks that allow a malicious virtual machine (VM) to compromise the hypervisor, as well as techniques used by the malicious VMs for hunting further allocation of physical resources, and strategies for bypassing the isolation between the VMs via side-channels. Side channel attacks bypass virtual machine isolation in the Cloud environment. The usage of CPU-cache based side-channels in the Cloud is investigated in [24].

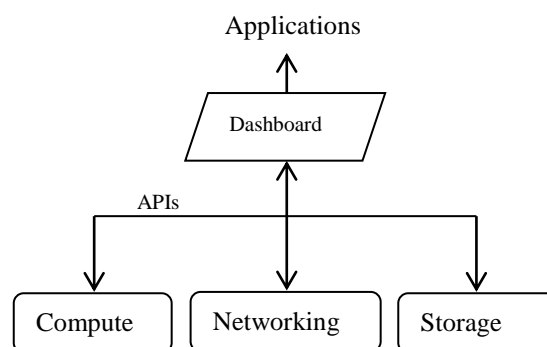
A block cipher mechanism is proposed in [25], to encrypt/decrypt Cloud messages for maintaining data privacy, based on the generation of a public key. The key is extended to be 3223 bits length, overcoming the hardware breakable key of length 512 bits. These threats are coming from the conceptual conflict among Cloud stakeholders, loss of governance due to privacy black-box provided, non-protected APIs, service provided lock-in, breakthrough of hypervisors, data loss and lack of cryptographic management, *etc.*

## 7. Experimental Experience

A complete private cloud environment has been established (NTI-MiniCloud) based on the open source platform 'OpenStack' (newton version), to proof the concept of Cloud computing (<http://docs.openstack.org/newton/install-guide-ubuntu/>). It consists of five nodes; namely, control, compute, block storage, and two object storages. A core i7 with 8 GB RAM and 1 Tera hard drive is used to install ubuntu 16.04 and the KVM hypervisor to explore VMs for hold the Cloud nodes (Hosted Virtualization).

The controller node runs the Image service, Identity service, management portions of Compute, management portion of Networking, and the dashboard. It also runs the SQL database, message queue, and NTP. The compute node runs the KVM hypervisor portion that operates instances. It also runs a Networking service agent that connects instances to virtual networks, providing firewalling services to instances via security groups. The Block Storage node contains the storage space for instances provisioning of the Block Storage and the Shared File System. The Object Storage nodes contain the space for storing accounts, containers, and objects.

The administration and management tasks is explored through a simple graphical interface; dashboard, to deploy the three main services; compute, networking, and storage, as shown in Figure 4.



**Figure 4. The OpenStack Environment**

The OpenStack Networking service is deployed in the simplest possible way, with primarily layer-2 (bridging/switching) services and VLAN segmentation of networks. DHCP service provides IP addresses information to virtual nodes as well as the provisioned instances.



## 8. Conclusion

As the business core of the Cloud computing is to deliver services, the providers deploy much robust infrastructure and supporting resources to meet the SLA. The reputation of the provider in this matter is critical as it differs from a provider to another. However, many organizations view reliability as a barrier because some Cloud providers tend to rely on commodity hardware that is known to fail. So that someone is encouraged to move to the Cloud environment, if (s)he could 1) have access to data and applications from around the globe (Availability), 2) benefit from the huge amount of information and resources available (Collaboration), 3) make use of the deploy and the release resources on demand bases (Scalability and Elasticity): 4) establish new projects without minimum initiation and maintenance costs (Lower Infrastructure Cost and Risk Reduction), 5) guarantee consistent service quality (Reliability). Finally, users should pay only for what are actually used, no extra fees. Hence, these drivers lead to the presented 360-degree reference to cover all Cloud computing issues, beginning from the components, deployment and management, market-share and revenue, ending up to standardization and research challenges and further work needed.

## References

- [1] M. Hamdaqa and L. Tahvildari, "Cloud computing Uncovered: A Research Landscape. *Advances in Computers*", Elsevier, vol. 86, (2012).
- [2] L.-J. Zhang and Q. Zhou, "Cloud computing Open Architecture", *International Conference on Web Services*, © IEEE (2009).
- [3] W.-T. Tsai, X. Sun, and J. Balasooriya, "Service-Oriented Cloud computing Architecture. *Seventh International Conference on Information Technology*", IEEE, (2010).
- [4] M. A. Chauhan, M. A. Babar, and Q. Z. Sheng, "A Reference Architecture for a Cloud-Based Tools as a Service Workspace. *International Conference on Services Computing*," IEEE, (2015).
- [5] J. Chawki. *Cloud computing Perspectives and Standardization. Workshop on "Developments regarding telecommunication network architectures and services," Kampala, Uganda, 2 April (2012).*
- [6] M. BaqerMollah, K.R. Islam, and S. S. Islam, "Next Generation of Computing through Cloud Computing Technology", *25<sup>th</sup> Canadian Conference on Electrical and Computer Engineering (CCECE)*, IEEE, (2012).
- [7] C. Delimitrou and C. Kozyrakis, "HCloud: Resource-Efficient Provisioning in Shared Cloud Systems," *ASPLOS '16, April 02-06, Atlanta, GA, USA* © ACM (2016).
- [8] X. Meng, CanturkIsci, J. Kephart, L. Zhang, E. Bouillet, and D. Pendarakis, "Efficient Resource Provisioning in Compute Clouds via VM Multiplexing", *ICAC'10, June 7–11, 2010, Washington, DC, USA, ACM*, (2010).
- [9] D. Ardagna, B. Panicucci, and M. Passacantando, "Generalized Nash Equilibria for the Service Provisioning Problem in Cloud Systems", *IEEE Transactions on Services Computing*, volume 6, no. 4, (2013).
- [10] V. D. Valerio, V. Cardellini, and L. Presti, "Optimal Pricing and Service Provisioning Strategies in Cloud Systems: A Stackelberg Game Approach," *Sixth IEEE International Conference on Cloud computing CLOUD*, (2013).
- [11] A. Jula, E. Sundararajan, and Z. Othman, "Cloud computing service composition", "A systematic literature review", *International Journal of Expert Systems with Applications*, Elsevier, (2014), pp. 3809–3824.
- [12] Y. Ma, H. Wang, J. Dong, Y. Li and S. Cheng. ME2, "Efficient Live Migration of Virtual Machine With Memory Exploration and Encoding," *International Conference on Cluster Computing*, IEEE, (2012).
- [13] W. Hu, A. Hicks, L. Zhang, E. M. Dow, V. Soni, H. Jiang, R. Bull, and J. N. Matthews, "A Quantitative Study of Virtual Machine Live Migration," *CAC'13, ACM*, (2013).
- [14] D. Armstrong, D. Espling, J. Tordsson, K. Djemame and E. Elmroth, "Contextualization: dynamic configuration of virtual machines. *Armstrong Journal of Cloud computing: Advances, Systems and Applications*, (2015).
- [15] A. Hans and S. Kalra, "A Comprehensive Study of Various Load Balancing Techniques used in Cloud Based Biomedical Services", *International Journal of Grid Distribution Computing*, vol.8, no.2, (2015), pp.127-132.
- [16] K. Al Nuaimi, N. Mohamed, M. Al Nuaimi and J. Al-Jaroodi, "A Survey of Load Balancing in Cloud computing: Challenges and Algorithms," *IEEE Second Symposium on Network Cloud computing and Applications*, (2012).

- [17] Qinghua Zheng, Rui Li, Xiuqi Li, and Jie Wu, "A Multi-Objective Biogeography-Based Optimization for Virtual Machine Placement," 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (2015)
- [18] Imran Ghani, NaghmehNiknejad, and SeungRyulJeong, "Energy saving in green cloud computing data centers: A review", Journal of Theoretical and Applied Information Technology, vol.74 no.1, (2015).
- [19] S.-Y. Jing, S. Ali, K. She, and Y. Zhong, "State-of-the-art research study for green Cloud computing," J. Supercomput, Springer, (2013).
- [20] T. Mastelic, A. Oleksiak, H. Claussen, I. Brandic, J.-M. Pierson and A. V. Vasilakos, "Cloud computing: Survey on Energy Efficiency," ACM Computing Surveys (CSUR), vol. 47, no. 2, article no. 33, (2015).
- [21] M. F. Al-Jaberi and A. Zainal, "Data Integrity and Privacy Model in Cloud computing", International Symposium on Biometrics and Security Technologies (ISBAST), (2014).
- [22] Y. Gu, Y. Fu, A. Prakash, Z. Lin and H. Yin, "Multi-Aspect, Robust, and Memory Exclusive Guest OS Fingerprinting," IEEE Transactions on Cloud Computing, vol. 2, no. 4, (2014).
- [23] A. R. Riddle and S. M. Chung, "A Survey on the Security of Hypervisors in Cloud computing," 35th IEEE International Conference on Distributed Computing Systems Workshops, (2015).
- [24] M. Godfrey and M. Zulkernine, "Preventing Cache-Based Side-Channel Attacks in a Cloud Environment," IEEE Transactions on Cloud Computing, vol. 2, no. 4, (2014).
- [25] Kangchan Lee, "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications IJSIA, vol. 6, no. 4, (2012), pp. 25-32.