iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

A Detailed Study on Cloud Computing Fundamentals and Security Issues

Kolluru Venkata Nagendra[1], Kavarthapu Sreenivas[2], N.Haritha[3]
[1]*Assistant Professor Department of CSE , Geethanjali Institute of Science and Technology,*
[2]*Assistant Professor Department of CSE GIST, Nellore.*
[2]*Assistant Professor Department of CSE SHIPS, Nellore*

Abstract: In Computer Science, the Cloud Computing is an emerging way of computing. The Cloud Computing has advanced computational power and improved storage capabilities. The computing techniques like Grid computing, distributed computing are also extends from Cloud Computing. Now a days the computational world adapting the technique pay-per-use. Virtual resource via internet was provided by the Cloud Computing to the uses of cloud. Currently sales force, Amazon and Google are providing Cloud services. There are so many issues still to be addressed in Cloud Computing. The objective of this paper is to explore different security issues and research opportunities.
Keywords: Cloud Computing, Cloud Security, Security Techniques, Cloud challenges and benefits.

I. INTRODUCTION

Cloud computing is another name for Internet computing. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. For some it is a paradigm that provides computing resources and storage while for others it is just a way to access software and data from the cloud. Cloud computing is popular in organization and academic today because it provides its users scalability, flexibility and availability of data. Also cloud computing reduces the cost by enabling the sharing of data to the organization. Organization can port their data on the cloud so that their shareholders can use their data. Google apps is an example of cloud computing. However Cloud provides various facility and benefits but still it has some issues regarding safe access and storage of data. Several issues are there related to cloud security as: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc. are some of the research problems in cloud computing [2]. In this paper we analyze the security issues related to cloud computing model. The main goal is to study different types of attacks and techniques to secure the cloud model.

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories. Infrastructure as a Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Our next section presents the Architecture of Cloud Computing. Section III and IV describes Benefits and challenges of Cloud Computing. Knowledge about various clouds discussed in section V. The next Sections VI and VII discuss the cloud security issues and Techniques to secure data in cloud. The discussion of Research issues in cloud present in section VIII. The commercial products of cloud mentioned in section IX, flowed by Conclusion. In the final section references are given.

II. CLOUD COMPUTING ARCHITECTURE

This section describes the layered model of Cloud Computing architecture.[3] This architecture of a cloud computing environment can be divided into 4 layers: the hardware/datacenter layer, the infrastructure layer, the platform layer and the application layer, as shown in Fig. 1. We describe each of them in detail:

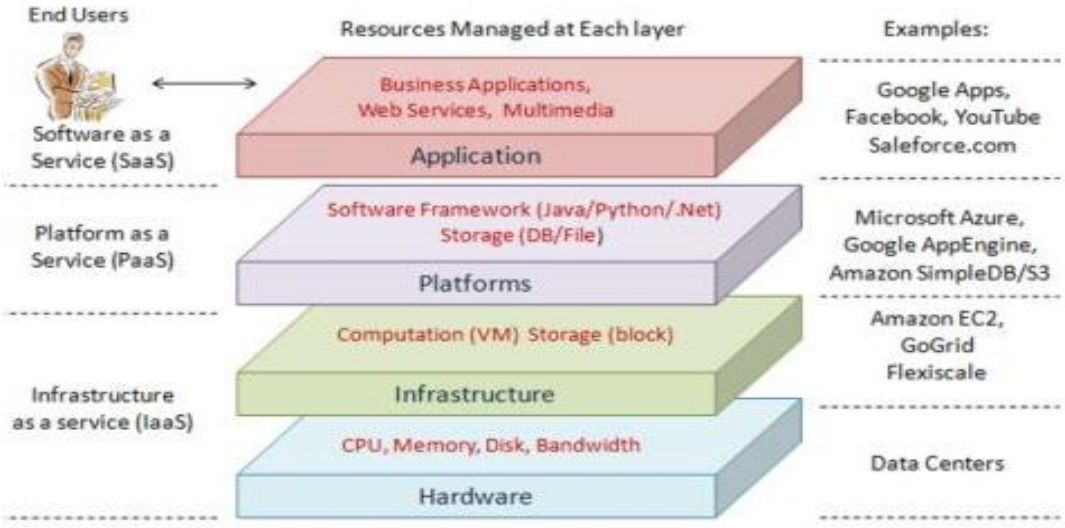


Figure 1: Cloud Computing Architecture

S.No	Layer	Responsibility	Implementation
1	Hardware Layer	This layer is responsible for managing the physical resources of the cloud, including physical servers, routers, switches, power and cooling systems	It is implemented in data centers
2	Virtualization Layer Or Infrastructure layer	The infrastructure layer creates a pool of storage and computing resources by partitioning the physical resources using virtualization technologies such as Xen [4], KVM [5] and VMware [6].	Its implementation is possible only virtualization technologies.
3	Platform Layer	The purpose of the platform layer is to minimize the burden of deploying applications directly into VM containers.[3]	It is used for implementing storage, database and business logic of typical web applications
4	Application Layer	The application layer consists of the actual cloud applications. Different from traditional applications, cloud applications can leverage the automatic-scaling feature to achieve better performance, availability and lower operating cost.	The different applications are implanted for different purposes.

III. BENEFITS OF CLOUD COMPUTING

Here is no doubt that businesses can reap huge benefits from cloud computing. The following are the some of the benefits of Cloud Computing.

A. Flexibility Cloud computing offers much more flexibility than past computing methods.
B. Reduced Cost Cloud technology is paid incrementally, saving organizations money.
C. Increased Storage Organizations can store more data than on private computer systems.
D. Highly Automated No longer do IT personnel need to worry about keeping software up to date?
E. More Mobility Employees can access information wherever they are, rather than having to remain at their desks.
F. Allows IT to Shift Focus No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation[7].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

IV. CHALLENGES IN CLOUD COMPUTING

The cloud is no longer just an interesting way to reduce IT costs. Today, it is about transforming businesses, gaining extreme competitive advantage, interacting directly with customers in real time, and dozens of other game-changing possibilities. Challenges to cloud adoption come in all shapes, sizes and severities, depending on the organization. None should be considered show-stoppers, but that doesn't make them any less real or significant. There is no definitive list of challenges; if there was it would be outdated as soon as it was put to paper. However, in speaking with prospective customers, attending tradeshows and working with clients on their future cloud roadmaps, there are recurring themes. The following are the challenges we hear most often.

A. Self-healing - in case of application/network/data storage failure, there will always be a backup running without major delays, making the resource switch appear seamless to the user.
B. Multi-tenancy - the cloud permits multiple clients to use the same hardware at the same time, without them knowing it, possibly causing conflicts of interest among customers.
C. Service-oriented - cloud allows one client to use multiple applications in creating its own.
D. Virtualized - applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program.
E. Linearly scalable - cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.
F. Data management- distribution, partitioning, security and synchronization of data.
G. Cloud date ownership - in the contract agreements it may state that the CP owns the data stored in the cloud computing environment. The CSP may demand for significant service fees for data to be returned to the enterprise when the cloud computing SLAs terminates.

V. TYPES OF CLOUDS

There are different types of Clouds available. Depending upon their cost, reliability and security the clouds are categorized as Public, Private, Hybrid and Virtual Private cloud etc.

A public cloud is one in which the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds. A public cloud is the obvious choice when standardized workload for applications is used by lots of people, such as e-mail.

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduce the cost savings.

A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds. [3]

Virtual Private Cloud is an alternative solution to addressing the limitations of both public and private clouds is called Virtual Private Cloud (VPC). A VPC is essentially a platform running on top of public clouds. The main difference is that a VPC leverages virtual private network (VPN)technology that allows service providers to design their own topology and security settings such as fire wall rules. [8]

VI. CLOUD SECURITY ISSUES

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has various cloud security issues. Each service model is associated with some issues. Security issues are considered in two views first in the view of service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is secure enough. The below Table:I provides the various security issues in Cloud Computing.

Table:I - The various security issues in Cloud Computing.

S.No	Security Issue	Explanation
1	Multi-tenancy	Multi-tenancy provides efficient utilization of resources, keeping cost lower. It implies sharing of computational resources, services storage and application with other tenants residing on same physical/logical platform at provider's premises. Thus it violates the confidentiality of data and results in leakage of information and encryption and increase the possibility of attacks
2	Elasticity	Elasticity is defined as the degree to which a system is able to adapt to workload changes by provisioning and deranged resources in an autonomic manner, such that the available resources match the current demand at any time as closely as possible. Elasticity implies scalability. It says that consumers are able to scale up and down as needed.
3	Insider attacks	Cloud model is a multitenant based model that is under the provider's single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees [1]. So a third party vendor can easily hack the data of one organization and may corrupt or sell that data to other organization.
4	Outsider attacks	This is the one of the major concerning issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network, they have more interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking. These attacks are less harmful than the insider attacks because in the later we sometimes unable to identify the attack.
5	Loss of control	Cloud uses a location transparency model by which it enable organizations to unaware about the location of their services and data. Hence provider can host their services from anywhere in the cloud. In this case organization may lose their data and possibly they are not aware about security mechanism put in place of the provider
6	Malware Injection	Attack Problem In cloud computing, a lot of data is transferred between cloud provider and consumer, there is a need of user authentication and authorization [9]. When the data is transferred between cloud provider and user, attacker can introduce malicious code into it. As a result, the original user may have to wait until the completion of the job that was maliciously introduced.
7	Flooding Attack Problem	In cloud, there is a no. of servers that communicate with one another and transfer data. The requests is processed, the requested jobs are authenticated first, but this authentication requires a lot of CPU utilization, memory and finally due to these server is overloaded and it passes its offload to other server[10]. By all this the usual processing of system is interrupted, and the system is flooded.
8	Data Loss	As in cloud, there are multiple tenants, data integrity and safety could not be provided. Data loss can results in financial, customer count loss for an organization. An important example of this can be updating and deletion of data without having any backup of that data.

VII. TECHNIQUES TO SECURE DATA IN CLOUD

The flowing are the some of the techniques to secure the data in Cloud.

A. Authentication and Identity
B. Data Encryption
C. Information integrity and Privacy
D. Availability of Information(SLA
E. Secure Information Management
F. Malware-injection attack solution.
G. Flooding Attack Solution

VIII. RESEARCH ISSUES IN CLOUD COMPUTING

A. *Availability of Service*

More availability problem is Distributed Denial of Service (DDoS) attacks Attackers makes use of large botnet's to reduce the profits of SaaS providers by DDoS by making their services unavailable [9]. A long botnet attack may be difficult to maintain, since the longer an attack lasts the easier it is to uncover and defend against, and on the same provide, these attacking bots could not be immediately reused for other attacks. These attacks are shifts by cloud computing to the Utility Computing provider from the SaaS provider. In this, who can more willingly absorb it and it also maintains DDOS protection in this competency

B. *Data Security*

1) Confidentiality, for secure data transfer and access,
2) Auditability, whether applications security setting has been tampered or not.
3) Cryptographic protocols, unencrypted data in a local data center in not secure compare to the encrypted data in before place into cloud.
4) Auditability can be achieved using remote attestation techniques and it could be added as an extra level away from of the virtualized guest Operating System, in one logical layer maintain some responsible software related to confidentiality and auditability.

C. *Traffic Management*

There is tight coupling of application's use to network, computing, and storage resources then what is present in other settings. Currently, the work on measurement and analysis of data center traffic is very less.

D. *Data Issues*

1) Cloud Computing users are more worried about increase in price, consistency problems, or even to providers leaving out of business. SasS developers could take the advantage of deploying the services and data on multiple Cloud Computing providers so that failure of a single company does not affect the customer data [10].
2) due to high workloads it is not easy to run extra tasks in private clouds compare to the public cloud
3) The applications are moved across the boundaries of clouds may complicate data placement and transport. Cloud providers and users have to feel about to minimize costs on the concept of the traffic and the implications of placement at each level of the system

E. *Performance Issues*

VM migration even though it is not straight forward. Initiating a migration lacks the facility to • respond to unexpected workload changes and • detecting workload hotspot. It should be transferred effectively in migrating process the workload in memory state. During the transfer it maintains consistency for applications by considering resources and physical servers.

IX. COMMERCIAL PRODUCTS

In this section, we providea survey of some of the dominant cloud computing products.

A. *Amazon EC2*

Amazon Web Services (AWS) is a set of cloud services, providing cloud-based computation, storage and other functionality that enable organizations and individuals to deploy applications and services on a non-demand basis and at commodity prices.
Amazon Web Services' offerings are accessible over HTTP, using REST and SOAP protocols. Amazon Elastic Compute Cloud (Amazon EC2) enables cloud users to launch and manage server instances in data centers using APIs or available tools and utilities. EC2 instances are virtual machines running on top of the Xen virtualization engine. After creating and starting an instance, users can upload software and make changes to it.
When changes are finished, they can be bundled as a new machine image.
An identical copy can then be launched at any time. Users have nearly full control of the entire software stack on the EC2 instances that look like hardware to them.

B. Microsoft Windows Azure platform

Microsoft's Windows Azure platform consists of three components and each of them provides a specific set of services to cloud users. Windows Azure provides a Windows based environment for running applications and storing data on servers in data centers; SQL Azure provides data services in the cloud based on SQL Server; and .NET Services offer distributed infrastructure services to cloud-based and local applications. Windows Azure platform can be used both by applications running in the cloud and by applications running on local systems. Windows Azure also supports applications built on the .NET Frame work and other ordinary languages supported in Windows systems, like C#, Visual Basic, C++, and others. Windows Azure supports general-purpose programs, rather than a single class of computing.

C. Google App Engine

Google App Engine [11] is a platform for traditional web applications in Google-managed data centers. Currently, the supported programming languages are Python and Java. Web frame works that run on the Google App Engine include Django, CherryPy, Pylons, and web2py, as well as a custom Google-written web application framework similar to JSP or ASP.NET. Google handles deploying code to a cluster, monitoring, failover, and launching application instances as necessary.

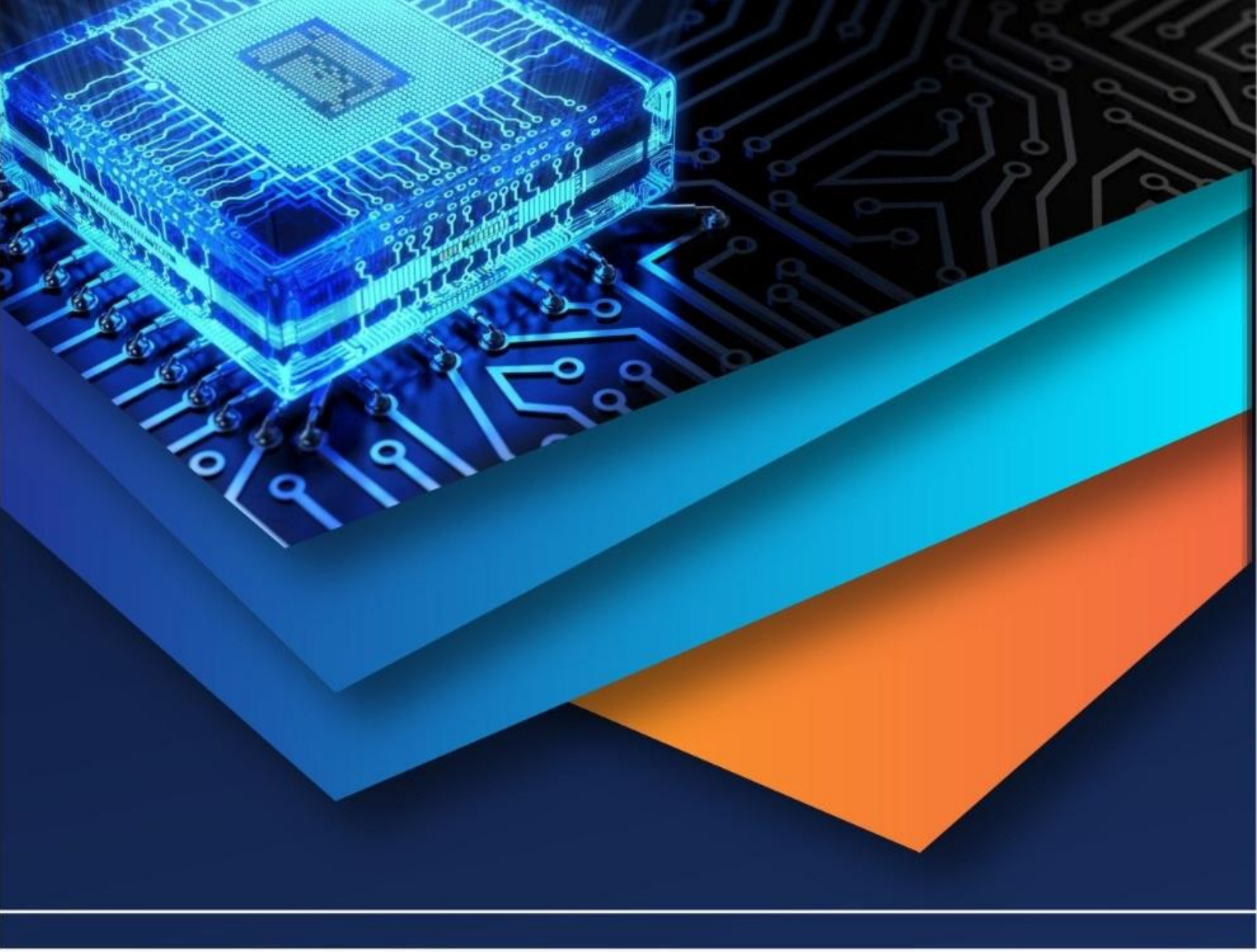
X. CONCLUSION

This paper describes the Cloud Computing concepts and demonstrates the security challenges. The Cloud Computing has a great advantage in the Information Technology. In this paper the detailed study of cloud gives the basic ideas for the Researchers to continue their research in various domains of cloud. The Research issue in the Cloud Computing provides a direct way to improve the quality in their work. Similarly, while storing the data in cloud the security plays a major role, this paper gives the security issues in detailed. In this paper a brief knowledge about commercial products and also gives pre requisitions of all the research.

REFERENCES

[1] Satyendrasinghrawat& Mr. AlpeshSoni (2012) ,A Survey of Various Techniques to Secure Cloud Storage.
[2] AkhilBehl&KanikaBehl (2012), An Analysis of Cloud Computing Security Issues.
[3] Qi Zhang,Lu Cheng and RaoufBoutaba,CloudComputing:State of art and Research Challenges, Springers J Internet Serv App-2010:7-18.
[4] XenSourceInc, Xen, www.xensource.com
[5] Kernal Based Virtual Machine, www.linux-kvm.org/page/ MainPage
[6] VMWare ESX Server, www.vmware.com/products/
[7] Geng Lin, David Fu, Jinzy Zhu, Glenn Dasmalchi "Cloud Computing: IT as a Service," presented at IEEE Computer Society conference in Beijing, 2009, pp. 10-13.
[8] Cloud Computing on Wikipedia, en.wikipedia.org/wiki/ Cloud Computing, 20 Dec 2009.
[9] R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing.
[10] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, BhavaniT,"Security issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April –June 2010.
[11] Aderemi A. Atayero, OluwaseyiFeyisetan, "Security Issues in Cloud Computing,The potential of Homomorphic encryption", Journal of Emerging trends in Computing and Information Sciences (2079-8407) , Vol – 2, P.No. 546-552. No.10 October 2011
[12] Chekuri C, Khanna S (2004) On multi-dimensional packing problems. SIAM J Comput 33(4):837–851Bhaskar P, Admela J, dimitrios K, YuesG ," Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach" Journal of Grid Computing 9(1), 3-26 , 2011.
[13] L. Ertaul, S. Singhal& G. Saldamli, Security Challenges In Cloud computing
[14] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009,
[15] Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA(European Network and Information Security Agency), Crete, 2009.
[16] Cloud computing security forum http://cloudsecurity.org/
[17] Cloud Computing – A Practical Approach by Velte, Tata McGraw- Hill Edition (ISBN-13:978-0-07- 068351-8)
[18] Yashpalsinhjadeja&kirtimodi (2012) cloud computing- concepts, architecture and challenges
[19] Liang-Jie Zhang and Qun Zhou."CCOA: Cloud Computing Open Architecture,"inProc.IEEE International Conference on Web Services, 2009, pp. 607-668.
[20] Lee Badger, David Bernstein, "US Government Cloud Computing Technology Roadmap", National Institute of Standards and Technlogy, Volume I, November 2011
[21] Cloud Computing on Wikipedia, en.wikipedia.org/wiki/ Cloudcomputing, 20 Dec 2009
[22] CloudHosting,CLoudComputingandHybridInfrastructurefromGoGrid, http://www.gogrid.com.
[23] Dean J, Ghemawat S (2004) MapReduce: simplified data processing on large clusters. In: Proc of OSDI
[24] Dedicated Server, Managed Hosting, Web Hosting by Rackspace Hosting, http://www.rackspace.com
[25] Flexi Scale Cloud Comp and Hosting, www.flexiscale.com
[26] Ghemawat S, Gobioff H, Leung S-T (2003) The Google file system. In: Proc of SOSP, October 2003.
[27] Google App Engine, URL http://code.google.com/appengine .
[28] Greenberg A, Jain N et al (2009) VL2: a scalable and flexible data center network. In: Proc SIGCOMM

[29] Guo C et al (2008) DCell: a scalable and fault-tolerant network structure for data centers. In: Proc SIGCOMM
[30] Guo C, Lu G, Li D et al (2009) BCube: a high performance, server-centric network architecture for modular data centers. In: Proc SIGCOMM
[31] Hadoop Distributed File System, hadoop.apache.org/hdfs 25. HadoopMapReduce, hadoop.apache.org/mapreduce
[32] Hamilton J (2009) Cooperative expendable micro-slice servers (CEMS): low cost, low power servers for Internet-scale services In: Proc of CIDR
[33] IEEE P802.3az Energy Efficient Ethernet Task Force, www. ieee802.org/3/az
[34] Kalyvianaki E et al (2009) Self-adaptive and self-configured CPU resource provisioning for virtualized servers using Kalman filters. In: Proc of international conference on autonomic computing.
[35] KambatlaKetal(2009)TowardsoptimizingHadoopprovisioning in the cloud. In: Proc of HotCloud [36]. Kernal Based Virtual Machine, www.linux-kvm.org/page/ MainPage.
[36] Krautheim FJ (2009) Private virtual infrastructure for cloud computing. In: Proc of HotCloud
[37] Kumar S et al (2009) vManage: loosely coupled platform and virtualization management in data centers. In: Proc of international conference on cloud computing.
[38] Li B et al (2009) EnaCloud: an energy-saving application live placement approach for cloud computing environments. In: Proc of international conf on cloud computing.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY