

Virtualization and Security in Cloud Computing

Shanu Khare¹, Mir Mohammad Yousuf*², Azhar Ashraf Gadoo³, Awadhesh Kumar Shukla⁴

^{1,3} Research Scholar , ,Department of Computer Science and Engineering, Lovely Professional University, Phagwara, India

^{2,4} Assistant Professor, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, India

Abstract- Cloud computing is the most prominent technology in today's world, as it can make less the cost value and problems or usage problems or complexity of applications. Cloud computing is capable of bending easily without breaking and it has an attribute that relate the potentiality or expertise of process, ability of network and software or organization to grow and managed increased demand. Cloud Computing is scalable because cloud computing is more adaptable to changing needs of its users. There are various advantages or profit gained by cloud computing that make changes in speedily growing technologies now a days. Cloud computing is going to be main identifiable part of the large internet or future developing internet. This technology Cloud computing is important to worthy of attention an event constituting a new stage in a changing situation. This is making practical and effective use of growing computational ability. Cloud Computing raises to a higher standards in data scattering and data storage facilities improve by adding or replacing components. It is extremely important details or facts to be saved in the cloud with the cloud information services. Virtualization means create or make a virtual version which is not the actual one it means create a version rather than actual. Virtualization is that term to define the quality of dealing with ideas rather than events it's all about to resources specially resources of computer. The action of making practical and effective use of resources or assets can be become well with the help of virtualization technology. This makes available for use the action or process of combination to the raised level surface on which user can stands. Virtualization gives the aggregation to the heterogeneous resources and the autonomous behaviour of the resources to the users and the customers.

Keywords: Cloud Computing, Virtualization, Security, CSP, CSA, CRM, Auditing.

I. INTRODUCTION

Cloud Computing is a very popular technology. It is begin to be in favour as virtualization power. Cloud Computing is also based on the give a share or a unit of computing to each of a number of recipients with collection of server or cluster of server. The quality of being able to be used an elevated-capacity communication methodology using only a broad frequency range that allow a significant number of signals to be transmitted concurrently with internet connectivity is that with the aid of cloud virtualization innovation [1][5]. A unit of information to each of recipient over number of users or customers. Cloud information is a central location in which data is stored and managed is involved with issues of information accuracy means data can't be altered whatever information is, that should be original, data security and information access by unauthorized users or customers[3]. Cloud Computing gives their users to access function separately and independently and also gives the information reviewing and auditing provision. These all provisions are needed to be done to fix that the details and facts are in such a manner as to achieve a desired such a convenient arrangements in the mist [7]. Cloud Computing is a basically demand based technique or technology in which there is existing a model or a framework for all the convenient and related access and also network access to distributed or shared of arrange or order computing resources so as to fit it for designated task[2]. Example of the arrange computing resources are- servers, networks, applications, storage and services. These assets or computing resources can be fast and swiftly allow to leave with minimal management services contributor interaction [2]. It means that simply where assets are virtual rather than actual there shared computing exists. Cloud Computing supports distributed and pooled amongst exterior data centres [21]. Data centres are accessible by the user through the internet or online facilities. Data centres are nothing but the database of all the information. In other words the data centres refers to the relative information and important information of the particular relevant data in the form of data bases where all the data and information is available. Cloud service provider provides all these services of the

cloud[13][15]. We can say that, these services related to the cloud provided by the one and only provider that is called CLOUD SERVICE PROVIDER (CSP)[9]. Cloud service provider should have to follow the all rules and best way to provide the services of cloud to the users or cloud customers. Cloud service provider should choose the acceptable and trustworthy manner or way for distributing the cloud services and also maintain the global rules or protocol of the global standards[20].

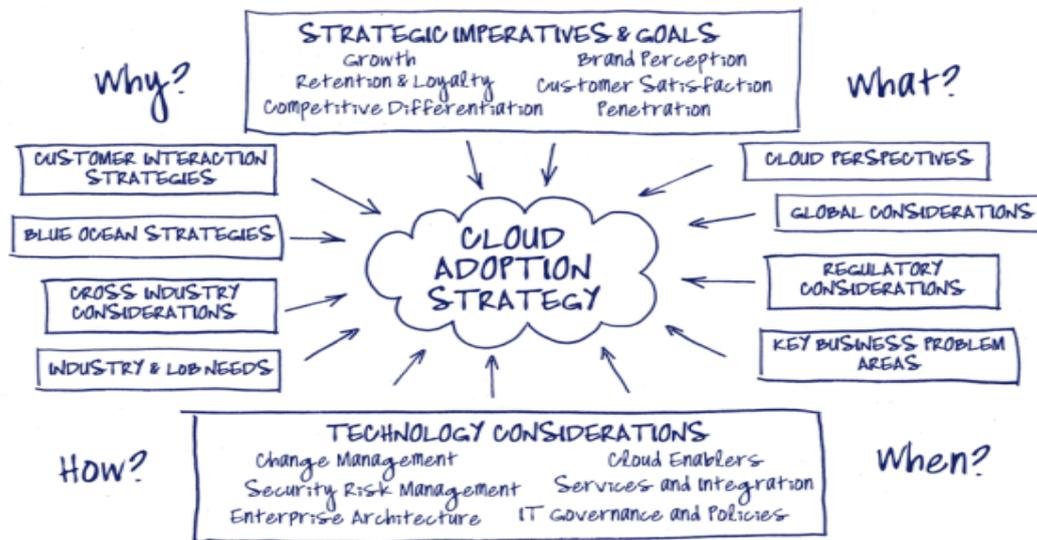


Fig 1. Strategy Adopted By Cloud Computing

There are three basic factor to define the term cloud computing or with these three factors we can say that this is the base of trending technology cloud computing are Autonomic Computing Grid Computing Utility Computing. Autonomic Computing is also called self-managing system. Autonomic computing is managed by self or user itself [12][13].

Autonomic computing depends on with full trust and confidence on monitoring examination or samples and indicators, device automation adjustment machine observational and analysis of information improvement or consistency across a dated of time, and deformers to perform system changes [16]. Grid computing gives the facility the formation of number of things into a cluster of the distributed resources and without the user being aware access them. Basically grid computing is an architecture which is distributed a large number of computers connected to resolve a difficult problems [17]. Utility Computing refers to fixed values which is called time varying values that captures different-different tasks. In utility computing users assign fixed values to perform the activities [19].

Cloud Computing has these three base factors which is very relatable and important term in this cloud technology.

Cloud storages are a huge collection of comfortably functioning and available virtualized possessions. These assets can be characterized by constant changing rearranged to amend to a mutable gauge of resources [6][17][18]. This collection of asset is in most cases utilized by a pay-per use architecture. This pay-per use protocol in which surely are presented by the substructure benefactor by revenues of modified Provision Level Contracts to suit a particular task of cloud computing. Pay-per use means nothing but the only concept is that provide the access only for those software or programs that are paid by users or customers [15]. With the help of Cloud computing, users can remotely access the all applications which are available in cloud or outside the network through devices which are using in connection of internet connectivity [4][5]. By this internet connectivity, computer assets can be organized in a way that achieves maximum productivity with minimum wasted effort or expense used and ingest less computing ability and assets are rationed in a way that involves mutual assistance in working towards a common goal. Cloud Computing is allowing also for an optimum resource utilization [10].

There are some elements of Cloud Computing. These are Data centres, Distributed servers, Clients

These are the basic components of cloud computing. Data centres are a group of servers where the application is provide. Data centres are the some kind of databases where all data are stored which is accessible by the users or customers. Where multiple virtual servers are created by instances, Virtualization is done. Distributed server

means that the server which are not inhabit locally but geographically. Distributed server refers to the multiple server collection. The data on each server can be similarly and parallel accessed and modified via network. The foremost goalmouth of cloud computing is to provide computing ability, storage backup and software “as a service”. Clients means Users. Users in the form of computers, desktops, mobile phones or PDA’s etc.

II. LITERATURE REVIEW

Anitha H M et al [1] in this paper talked about the security provocations of virtualization in cloud domain. All the services of the cloud computing are associated to the virtualization technique. Such as platform as a service, infrastructure as a service, software as a service, network as a service and one more service is there which is totally depend on the virtualization that is called virtualization as a service. In this particular paper, author said that the security challenges how to effect the cloud virtualization and what type of security issues faces by the users and customers of cloud environment. The security of virtual machines have already looked up with the high priority and preferences. The risk is major critical asset in the virtualization in cloud computing and its mitigation at that virtualized level are watched by the surveyed. In this paper, various weaknesses of the security are recognized and existing or occurring now different-different algorithms by the protocol and rules and applied proceed towards to provide security to layer of virtualization.

T. Swathi et al [2] in this paper talked about basically two types of controls in the cloud computing domain one is physical control and the other is virtual control. In the cloud, must have to implement and use the encryption techniques. With the help of encryption technique, can encrypt the data or information and can secure and protect the communication media which exists in between client and the cloud server. One benefit is there of encrypted data that is data loss prevention. For data loss prevention we can apply the prevention policies. Access control policies are also available for checking the user authentication and for security from the unauthorized access.

Malhotra L et al [3] in this paper talked about the basic problem and challenges faced by users to use the cloud computing virtualization application. And also talked about the basic thing is how the cloud computing is succeed in dealing with some problems of losing the data, accessing the data and the safekeeping of data. Cloud machinery is the application of scientific knowledge which is about reduction of some important assets. Such as reduction of cost, reduction of hardware, and the reduction of money also. Cloud computing is working these concepts only. Virtualization is basically used in cloud computing for sharing the resources and creating the isolation image that is also called an imaginary image or virtual image which is not actual. Virtualization is used in cloud computing for one more reason that is dynamically resource allocation. In this paper author talked about some issues of virtualization in cloud computing. These issues can be fronted by using virtualization type of scientific knowledge. Those issues are-

- a. Infected application
- b. Accuracy of the data
- c. Mass data loss

Farzad Sabahi [4] in this paper talked about one technology related to the virtualization named as Hyper-visor which helps to secure the environment of cloud computing technology. In this paper gave a proposal virtualized architecture for securing cloud. In this proposal architecture author tried to explained some terminologies which helps to secure the virtualization in cloud computing. These terminologies are-

- a. Reduce the workload
- b. Decentralized security related tasks between hyper-visor and virtual machines
- c. Distribute the centralized security system or converting concepts indeed

Centralized system has minimal weaknesses as compare to distributed system. One advantage is to define the distributed system is good that is called fault tolerance. In this paper author said that whatever created by human in this computer world that can be breakable also. That’s why attacks are possible in the cloud era. Because of its vulnerability and in some situation their centralized concept creates an issue. However, the basic thing or concept is the decentralized application access creates a security problem in cloud computing environment that

can create major issue or problem while data transferring in cloud. So depending all the security perspective, have to manage the security of cloud computing environment and virtualization in cloud environment also.

LaQuata Sumter et al [5] in this paper talked about the basic scope of “Internet Security” in “Cloud Computing”. Also talked about the vulnerability in cloud computing which are increasing fast day by day. Each user has bother about server for security and entrance protocol or methods of cloud computing domain. For surety of the user, authors proposed a device arrangement of system that will seize gesture or move and moving transformation of the data or valuable data remained on the domain of cloud computing. This proposal is only for the small scale cloud framework not for large scale cloud domain. It is definitely used for provide security assurance to the users while communicating through the cloud domain or environment.

Mladen [6] this paper refers that the networking environment in the cloud computing overall area. This technique utilizes Security Oriented Architecture. With the help of Security Oriented Architecture domain can do the various tasks. Such that-

- a. Reduce the operation of information technology
- b. Preservation cost for the users of cloud computing applications
- c. It provides greater quality of bending easily without breaking
- d. Less capital cost
- e. Gives needed services

This paper talked about the vulnerability of using virtualization in cloud computing. It gives the some issues in cyber infrastructure also. This paper discussed issue about the Security issue in security oriented architecture and the client. This is a review paper basically. There is not any implementation work or working feedback about this paper. This creates a case study only which gives or provides us to overview with concern of issues related to technology using in cloud computing by the end users or customers or clients.

Soren et al [7] in this paper, authors concern about the misconfiguration in cloud platform by the users side or by the end users. When user accesses the web portal which is exist in the cloud platform and there is something misconfigured by mistake then it creates a weakness of the path or communication. This scenario can create an access for unauthorized party or users. This is all happen because of complexity and flexibility of cloud computing environment or domain. This paper proceeds towards presented for examining security at both the ends means user or client end and server end. For whole process of analysing they have been chosen Amazon’s Elastic Compute Cloud (EC2). In this procedure they proposed policies and security analysis like assessment mitigation auditing all the scenarios performed. They gives the security tools which provides assurance for the weakness and attacks on the security server cloud domain.

Flavi and Roberto [8] in this paper authors discussed about the accuracy prevention system in the cloud. This is very common and famous issue in cloud because of their complexity and weak configuration. Also gives review about TCPS (Transparent Cloud Protection System) for enhancing the security of cloud computing domain or environment. The Transparent Cloud Protection System is a system that was proposed by the authors for increasing and developing security in cloud computing environment. This security breach came because of integrity or accuracy prevention problem of data in cloud computing domain. In this system, whoever the unregistered user tries to access the cloud computing applications in between the accuracy of the data or the information and remain the condition of being transparent data and virtualization.

Wayne [9] in this paper, author talked about the problems of security matter in the security services with their benefits which are still exist in cloud domain. For the condemnatory systems, configuration is very difficult and necessary. This paper is basically defined the preliminary issues in cloud configuration and basic connection between end user to server or cloud server. The main problem discussed by author in this paper is that the public cloud model. Public cloud is an accessible platform for everyone so there is some issues related to the security and trusting parties. End users cannot create proper trust in this interface because of their security reasons. So for all these problems proposed a key focused system which was manage all these problems. Such that-

- a. Visibility
- b. Identity management
- c. Untrusted party

- d. Insider access
- e. Server side protection
- f. Risk management
- g. Users side protections
- h. Access control management

Table 1. Summary of the review in collate and disparity table

List Ref	Context of Research	Problem Discussed	Technique Used	Model/ Tool/ Proposed
1.	Security Provocation of Virtualization in Cloud Environment	Various security challenges of virtual machines on all platforms of cloud	Research Theory In	No
2.	Virtualization In Cloud Computing	Control Policies in Cloud Computing	Research Theory in	No
3.	Virtualization In Cloud Computing	Data Security and Accessing Data with high cost	Research Theory in	No
4.	Secure Virtualization For Cloud Computing Using Hyper-Visor Based Technology	Difference between centralized and decentralized system	Secure Virtualization Architecture In Cloud Computing	No
5.	Trusted Cloud Computing	Safekeeping Prospect and recruit of Retreat to cloud patrons	Trusted Computing Platform (TCCP)	Yes
6.	Implementation And Research Issues in Cloud Computing	SSH passageways and VLANs, provable exactness of data and end-to-end provision connectivity concluded Simulated procedures	Virtual Computing Lab (VLC) technology, open source	No
7.	Security Audit in Public Infrastructure clouds	Horizontal scrolling Review of Amazon Security Groups & People	Amazon's Elastic Compute Cloud (EC2)	Yes
8.	Transparent Cloud Services	Cloud Security flaws and	The Transparent Cloud	Yes

		Safekeeping Spells	Protection System	
9.	Security And Privacy in Cloud	End consumer faith, internal authentication, transparency, internal controls, security of the local machine, protecting of the server side, distinctiveness management and admittance control	Research In Theory	No

III. METHODOLOGY

In Methodology section, there is two basic methods related to cloud computing domain. Without them cloud computing does not exist anymore because all the process and procedure happens in cloud computing platform those are related to these two. Cloud Computing is a platform only which provides new technique with the proper access to the client or end user. Accessing all applications on cloud and be with the cloud when it gives something important. All because of –

- a. Virtualization in cloud computing
- b. Security of virtualization in cloud computing

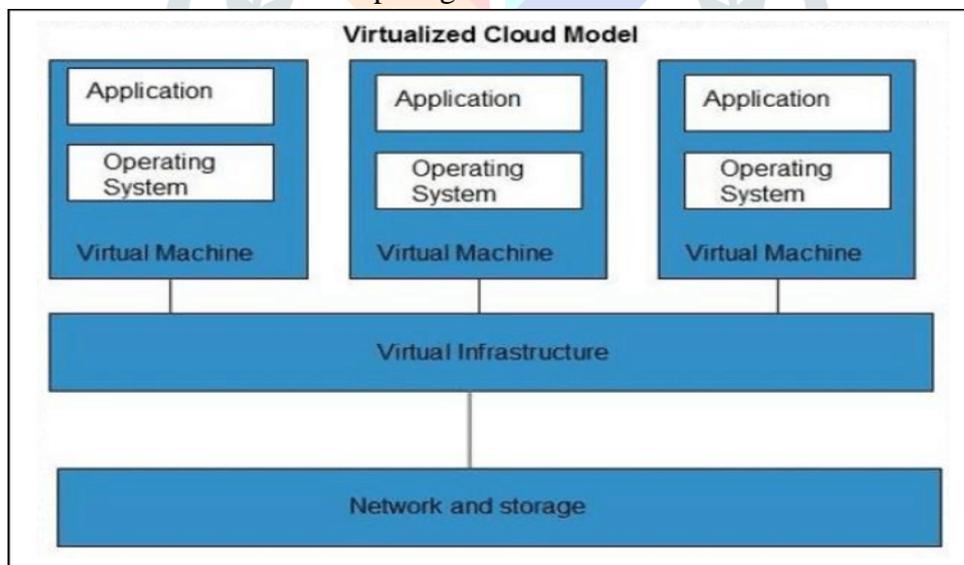


Fig 2. Virtualization in Cloud Computing

a. About The Virtualization in Cloud Computing

Virtualization is a virtual technique which exists virtual rather than actual. It gives access to the clients virtually not physically. Virtualization provides to distribute one concrete occurrence of assets between the many organizations. Virtualization is an abstraction layer that is also called as Hypervisor that separate materials hardware from the operating system to provide best IT assets utilization and flexibility [6]. Virtualization also allows many virtual machines with the same type of operating system execute in separation side-by-side on the same physical machine. In general term, there are some benefits of the virtualization service infrastructure. These are-

- a. Save Money
- b. Dramatically Increased Control

- c. Simplify Disaster Recovery
- d. Business Readiness Assessment
- e. It can change their strategy depends upon organizational structure

i. Why Virtualization?

In virtualization, all about the environment or can say virtual environment which is logically isolated from an underlying hardware. In virtualization, concepts depends on the two types of machines. These are-

- a. Host Machine
- b. Guest Machine

Host Machine is that machine which is act like a virtual or which machine on that the virtual machine is created that is called as a Host machine.

Guest Machine is that machine which is generally virtual machine.

The Virtual Machine is generally be head of a software which is called as hypervisor. Hypervisor is a layer which is abstract the data and information. Virtualization is a basic technique which is basically used for reduce the complexity of adding to that infrastructure service provided by the cloud computing framework. Virtualization can create a same type of networking infrastructure for capturing the response of organizational review [9].

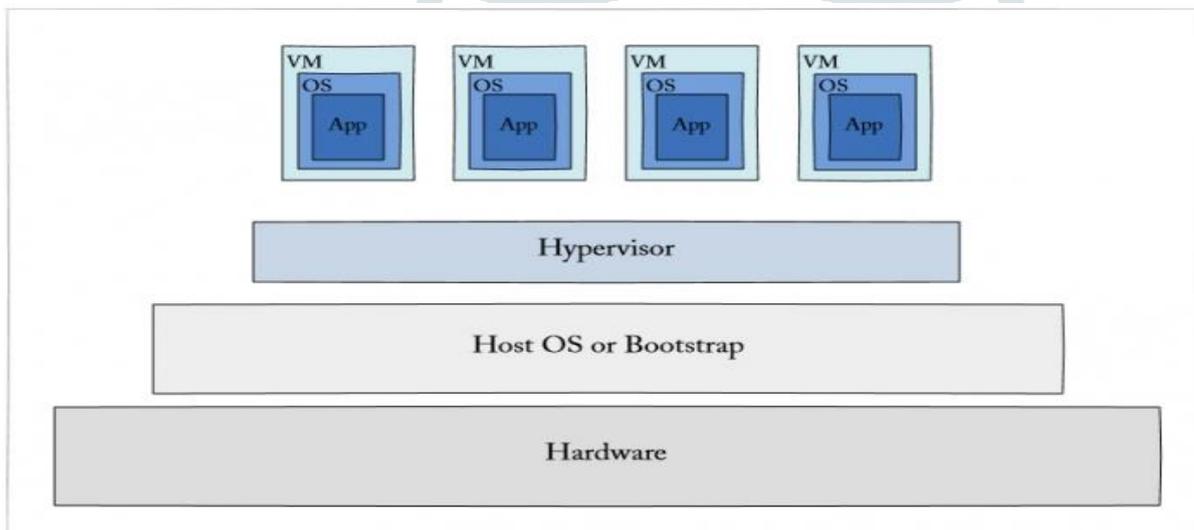


Fig 3. Layers of Virtualization

ii. Virtualization Technology

With the help of virtualization concepts, user gets the better infrastructure of virtualization to be implemented. All the benefits of virtualization which permits automatic supplying of domain and deployment of applications into those beneficial domain related to virtualization [1]. Virtualization has a power to create self-service like-

- a. Provisioning
- b. Scaling
- c. Monitoring
- d. De-provisioning

There are three main purpose for using virtualization technology. These purposes are-

- a. Storage Virtualization
- b. Server Virtualization
- c. Network Virtualization

Storage Virtualization is nothing but a storage media which works like a central device for all network connecting resources and devices. This is directly related to the storage area network concept [2]. Virtualization as a server is nothing but enabling the server assets like CPU, RAM, Operating System etc. which provides server end connectivity and required connection from receiver end also. The important goal of the server virtualization is to enhance the device sharing, reduce the large scale complexity form users [2]. Virtualization as a network is nothing but a technique to merge all available assets in a network by separating the available bandwidth into channel. In this virtualization, each and every device or resource works independently from

others these are not dependent any other resource or device. Similarly channel which works independently from other channels also [2].

About The Security in Cloud, in the cloud computing platform security is a biggest issue. For security reasons in case of data or information security there should be encrypted form takes place. All type of data in cloud have to be encrypted. There should be a rule to follow by all the customers that restriction to authorize shared data directly. Virtualization and security both are maintained a relationship in between customer and service provider and produced a model to define the boundaries. There is a models to define their limitations [3]. That is called- Cloud Security Alliances (CSA)

Cloud Security Alliance (CSA) is a stack type of model which is follow the rules and protocols of stack only. This model provides the limitations of each and every service model and display the multiple function related to in between.

IV. CONCLUSION

Cloud computing basically is a framework which provides access of the application with the help of virtualization technique. User or client can do multiple work on the cloud with the help of virtual machines. Such that sharing data, communication, access the applications. Cloud provides the access on pay per use rule or protocol. Term of application prise paid by user or client. User can faced the problems in security field of cloud computing. In this framework, apply multiple security methods can provide the security by the security management. Virtualization technology is one of the technology which helps to secure the sensitive and important data. Cloud computing is a storage framework which stores the private data as per customer demand. Whatever the application purchased by user it can access by the authorized user only. In Cloud Computing, there are some vulnerabilities also. Basically cloud always deal with the threat in the server area because of its complexity in the configuration. There is need to be secure the connectivity path for data of user security. Security issues are in any type and any shape so that all risk mitigation rules must be enable for the user to secure their application and secure their account on cloud. In future, the storage system of world will depend only on the cloud, and there will be multiple obstructive and computational device based and storage based problem occur. The work has to be done in order to support cloud computing and virtualization and also understanding the challenges regarding security issues in cloud.

V. REFERENCES

- [1] Anitha H M , P. Jayarekha, International Journal of Scientific Research in Computer Science and Engineering, Security Challenges of Virtualization in Cloud Environment, Vol.6, Issue.1, pp.37-43, Feb (2018)
- [2] Malhotra L, Agarwal D and Jaiswal A, Journal of Information Technology and Software Engineering, Virtualization in Cloud Computing, 2014, 4:2 DOI: 10.4172/2165-7866.1000136
- [3]R. La'Quata Sumter, Cloud Computing: Security Risk Classification, ACMSE 2010, Oxford, USA
- [4] Mladen A. Vouch, Journal of Computing and Information Technology, Cloud Computing Issues, Research and Implementations, CIT 16, 2008, 4, 235–246
- [5] Soren Bleikertz, Matthias Schunter, Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds, CCSW 2010, Chicago, USA.
- [6] Flavio Lombardi& Roberto Di Pietro, Transparent Security for Cloud, SAC'10 March 22-26, 2010, Sierre, Switzerland.
- [7] Wayne A. Jansen, 44th Hawaii International Conference on System Sciences, Cloud Hooks: Security and Privacy Issues in Cloud Computing, 2011.
- [8] Jinpeng, Zhongshan, Guangdong, Managing Security of Virtual Machine Images in a Cloud Environment CCSW, 2009, Chicago, USA
- [9] Dr. Kumar Saurabh (2013) Cloud Computing Second Edition (Wiley-India)
- [10] T.Swathi, K.Srikanth, S. Raghunath Reddy (2014), International Journal of Computer Science and Mobile Computing, Virtualization in Cloud Computing, IJCSMC, Vol. 3, Issue. 5, May 2014, pg.540 – 546.

- [11] Ashima Narang, GE-International Journal of Engineering Research, Virtualization Security Management, Vol. 5, Issue 5, May 2017.
- [12] Farzad Sabahi, International Journal of Machine Learning and Computing, Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, Vol. 2, No. 1, February 2012
- [13] Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009. Available Online at: <https://cloudsecurityalliance.org/csaguide.pdf> (Accessed on: November 29, 2012)
- [14] IBM Blue Cloud Initiative Advances Enterprise Cloud Computing. URL: <http://www03.ibm.com/press/us/en/pressrelease/26642.wss>. (Accessed on: November 20, 2012)
- [15] Song, D., Wagner, D., & Perrig, A. (2000). Practical Techniques for Searches on Encrypted Data. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, pp. 44-55, May 2000
- [16] Zetter, K. (2010). Google hackers Targeted Source Code of More Than 30 Companies. Wired Threat Level. January 13 2010. Available online at: <http://www.wired.com/threatlevel/2010/01/google-hackattack/> (Accessed on: November 29, 2012)
- [17] International Organization for Standardization, <http://www.iso.org/iso/home.htm>
- [18] Information Technology Infrastructure Library, <http://www.ital-officialsite.com/home/home.asp>
- [19] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCS, Bangalore 2009, pp. 109-116.
- [20] Cloud Security Alliance (CSA). Available: <http://www.cloudsecurityalliance.org> [Mar.19, 2010]
- [21] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment> [Jul. 10, 2010]

