International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Novel and Integrated Assessment of Security Challenges in Cloud Computing

Mohd Muntjir[1], Mohd Rahul[2]

[1]Taif University, College of Computers and Information Technology, P.O. Box 888, Al-Hawiya Taif, Zip Code 21974, Saudi Arabia

[2]Taif University, College of Computers and Information Technology, P.O. Box 888, Al-Hawiya Taif, Zip Code 21974, Saudi Arabia

Abstract: ***Cloud computing is a technology that uses the Internet and central remote servers to preserve data and applications in a system. It also allows patrons and enterprises to utilize applications without installation and access their individual files with accessing the Internet at any computer. It also allows for much more well organized computing by centralizing data storage, bandwidth and processing. Within the last few years, Cloud computing has progressed as an important prototype for IT enterprises along with inexpensive in costs, transaction according to makes use of, scalability, quick ease of access along with more elasticity. Utmost undersized, medium and huge scale companies, organizations are moving towards cloud computing as it eliminates setting up of high-investment on IT communications and other services like Paas, NaaS and SaaS. In this system, the client data can be accessible in all around the world, controlled and maintained outside their accessibility. Accordingly, there can be privacy and security issues with the client's data. The services providers in cloud industry should convince their clients by ensuring and providing security to their accessible data. Hence, in this survey paper we present and examine different security and privacy issues obtainable in cloud computing. We have also discussed different security models top cloud service providers. Cloud computing system is consuming the globe, and each day is bringing innovative developments in this world.***

Keywords: Cloud Computing, Virtualization, IaaS, PaaS, SaaS, VMs (Virtual Machines), Multitenancy

1. Introduction

Cloud computing is one of the most emerging IT paradigm in recent times. This technology has made Everything-as-a-service enterprise model. This is a latest state of the art technique which works on pay-as-you-use model for all IT operations like providing platform services, infrastructure services, software application services etc [1]. In the simplest way cloud computing means storing and retrieving data and databases over the Internet instead of our computer's hard drive. Data storage on a home or office network does not mean as operating the cloud system. For it to be measured "cloud computing," we want to approach our data or our programs over the network, or at very minimum, have that data coordinated with other information over the Network. In some big enterprises, we may recognize all there is to know about what's on the other side of the network. The cloud computing is a blending of Business enterprise applications, data storage, Internet, management and networking and solutions. This technology provide enormous benefits like 1) scalable data solutions as per your business requirement, 2) reduced cost on infrastructure to put your money at another areas, 3) high accessibility because of accessing everything through internet, 4) backup and recovery of the your data becomes easier than earlier and 5) it also provides a quick deployment of the technology you need [2] [3]. Cloud Computing has been defined by US National Institute of Standards and Technology (NIST, http://nist.gov/itl/cloud) as follows: "Cloud computing is a model for supporting convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, different servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model help to provide availability and is composed of five essential characteristics (On-demand self-service, Resource pooling, Broad network access, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Public cloud, Community cloud, Private cloud, Hybrid cloud etc.).

The main technologies include:

(1). Fast WAN (Wide Area Network)
(2). Powerful, inexpensive and high performance Servers
(3). High performance virtualization

Cloud computing is the next big wave in computing. Cloud computing having lots of benefits, as better Software and hardware management, since all the computers are the same and run the same hardware. It provides better and easier management of data security and availability, since all the data is located on a central server, an administrator can control who have access to the files. (31).The end result is the same: cloud-computing system can be done anytime, anywhere, with an online internet connection.

This paper familiarizes the existing state of cloud computing system, through its improvement experiments, academia and industry research determinations. Further, it explains cloud computing security problems and benefits and platforms a model of secure architecture for cloud computing applications. The statistic that cloud computing is not used for all of its prospective is due to a diversity of apprehensions.

2. Cloud Computing Service Models

Cloud computing offers different types of services depending on business requirement, but mainly three

layers constitute the service model which are described as follows:

2.1 Infrastructure as a service (Iaas):

IaaS incorporates necessary services such as data storage, virtual servers, and databases into one platform for running and organizing applications. This forms a bottom layer of the service model, which provides a basic hardware and network support services. Italso provides platform for aggregating and maintaining the resources and which can also be scaled up or scaled down dynamically on-demand. IaaS is easy to spot, because it is usually platform-independent. IaaS comprises of a combination of hardware and software properties. IaaS software is low-level code that runs autonomous of an operating system—called a hypervisor and is accountable for taking inventory of hardware resources and dealing said resources based on needs. There may be many users using the resources parallel, which is accomplished by a billing depending upon the usage of the resources allocated [4]. The virtualization should be potentially superior so that the accessing thousands of virtual machines at a time with fast speed could be made possible. e.g. Amazon EC2, Google FS, Open Flow, HadoopMapReduce, Google Bigtable, Rightscale etc. [6].Most use cases for cloud computing follow the same fundamental layering structure we are already used in IaaS.

2.2 Platform as a Service (PaaS):

PaaS is distinctive in that it facilitates developers to establish and utilize web applications on a hosted organization and permits them to control the apparently immeasurable compute properties of a cloud computing organization. This middle layer comprises of the operating systems and middleware applications. This mainly offers developers a software development management platform to work on the lifecycle of application development with all the steps like designing, developing, testing to organizing [5]. Conclusively, it offers an application development and execution environment for developers. e.g. Google App Engine, Django, Microsoft Azure, Amazon SSS etc [6] [7]. In other words, PaaS acknowledges you to control the apparently infinite compute resources of a cloud computing organization.

2.3 Software as a Service (SaaS):

SaaS specifies network-based access to commercially accessible software and can lead to improved speed of software utilization, faster user approval of software, fewer support necessities, and improve in execution and advancements. SaaS also denotes the prospective for a lower-cost way for productions to use software; using it on requirement rather than procuring a license for each and every computer, exclusively when you believe that most computers assemble unused. This is a top layer of the cloud computing service model, which provides pay-per-use model for users on the Internet without bothering about the software deployment and continuance, as it is not installed on user's local computer. There is still a security concerns over the enterprises data the way they are stored and secured. e.g. Google docs, Salesforce.com, Opensocial, net suite [6][8]. SaaS applications also characterize a sort of next-generation methodology to application purpose. Though it might not be technologically specified in any of the credentials that I have seen to date, it appears that SaaS platforms also incorporate a recent methodology to UI design that is more reliable with the product design process seen in most other businesses. This approach contains a process known as user experience design (UXD), wherever a product team rather than the development team designs the GUI.

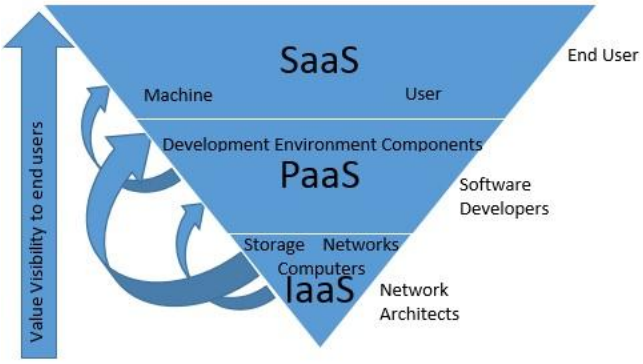
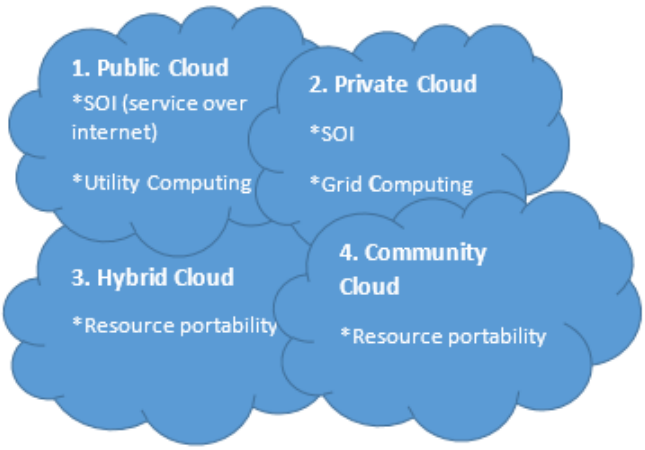


Figure 1: Cloud Computing Service Models

3. Cloud Service Deployment Model

Through cloud computing technology, large collections of resources can be connected through private or public networks. This technology streamlines organization planning and delivers vigorously accessible arrangement for cloud based data, purposes, and file storage. Productions can indicate to organize applications on Public, Private, Hybrid clouds or the newer Community Cloud. These deployment models depending on the customer's requirement like some customers mainly concentrates about security, some prefer low infrastructure cost:



3.1 Public Cloud:

A service provider who hosts the cloud infrastructure makes public clouds available to the general public. Usually, public cloud providers like Microsoft, Amazon AWS, and Google own and control the organization and offer approach over the Network. In public cloud, User is not bothered about investing on infrastructure as it is availed by Third-party cloud service provider [9]. They need to bill as per use of the services. So many users use the infrastructure provided at the same time. Cloud

Services are basically accessed through web browser on Network. This type of clouds offers the maximum level of competence in distributed resources; though, they are also more vulnerable than private clouds.

3.2 Private Cloud:

Private cloud is cloud infrastructure dedicated to a specific association. Private clouds acknowledge productions to host applications in the cloud, whilst addressing apprehensions concerning data security and control, which is regularly deficient in a public cloud atmosphere. It is not shared with other associations, whether managed internally or by a third-party, and it can be hosted internally or externally. This cloud is provided to specific customer and it can be managed either by the customer itself or third-party service provider [10]. This provides more security and reliability because it is availed and managed by the organization internally whereas public cloud is made available for so many customers. Responsibility a private cloud project necessitates a suggestive level and degree of engagement to virtualize the commercial atmosphere, and it will involve the organization to reassess assessments about accessible possessions.

3.3 Hybrid Cloud:

Hybrid Clouds are an arrangement of two or more clouds (private, community or public) that persist unique objects but are compelled together contribution the benefits of several deployment models. In this cloud, we can leverage third party cloud contributors in either a full or restricted manner; accumulative the elasticity of computing system. Intensifying a conventional private cloud with the resources of a public cloud can be used to accomplish any unanticipated flows in workload. Although, Hybrid cloud architecture involves both on-premise resources and off-site server based cloud organization. By spreading things out over a hybrid cloud, we keep each phase of our corporate in the most effectual environment potential. The obstacle is that we have to keep track of numerous cloud security platforms and confirm that all features of commercial can interconnect with each other's [7].

3.4 Community Cloud:

A community cloud is a multi-tenant cloud service model that is distributed among several organizations and that is managed, accomplished and protected commonly by all the contributing administrations or a third party managed service provider. Furthermore, a community clouds are a hybrid form of private clouds built and functioned exclusively for a pointed group. These communities have analogous cloud necessities and their decisive objective is to work organized to accomplish their commercial purposes. The main objective of community clouds is to have contributing organizations recognize the remunerations of a public cloud with the added level of security, privacy, and policy observance generally connected with a private cloud. Community clouds can be either on-premise or off-premise. A community cloud system is best at Government organizations within a state that need to share resources, a private HIPAA submissive cloud for a group of hospitals or clinics and Telco community cloud for telco DR to meet precise FCC procedures.

4. Security Issue of Cloud Computing

If you are using Word, use either the Microsoft Equation Editor or the MathType add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation or MathType Equation). "Float over text" should not be selected. The recent development of cloud computing has significantly improved everyone's awareness of infrastructure designs, software distribution and improvement representations. Maximum-security problems stem from Loss of control, Deficiency of trust (mechanisms) and Multi-tenancy. These complications exist mainly in 3rd party administration models. We can divide security issues of cloud computing at three distinctive levels:

4.1 Security Issues in IaaS:

4.1.1Impact of Cloud deployment model: The security needs for using Infrastructure as-a-Service are basically the same as they would be for using your specific data center. The IaaS layer is also vulnerable due to network and Internet connectivity associated with it. It is more prone in public cloud compared to private cloud. Physical security of infrastructure is also required for any disaster happening. The data transmission path is also needed to secure as the intruders can easily attack the data communicating between sources to destination [11]. The data flowing over the Internet is a major concern as the client and service providers are placed at two different locations, which are connected through Internetonly. Therefore it needs high encryption techniques and strong secures protocol to safeguard data transmission.

4.1.2Virtualization:

Virtualization developed extensively in the early 2000s, more years before the growth of cloud computing. Virtualization provides many features to the users to create, share, migrate, copy, rollback virtual machines which helps in running many applications on them [12, 13]. But, it also becomes prone to get attacked because it

opens more entry for the attackers and interconnected virtual machines complexity [14]. Virtual machines should also be considered as important as any other physical device security. Complete virtualization is comprehensive simulation of the hardware's.

4.1.3Hypervisor:
A hypervisor is a hardware virtualization procedure that consents several guest operating systems (OS) to run on a single host system at the same time. This is also called as Virtual Machine Monitor (VMM). This software is responsible for monitoring and controlling its virtual machines, so it clouds also produces some security flaws [14]. We can reduce security risks by keeping Hypervisors simple and less complex to easily trace and resolve security issues. The hypervisor program connected on the computer permitted the allocation of its memory.

4.1.4Shared storage resources:
To get highly available, redundant and high-performing storage for our physical or virtual systems, we need Shared storage resources for virtualization. Virtual machines are connected with same server. So, there is strong chance that if malicious virus affects one virtual machine, it can be used to monitor other Virtual machines shared resources. So, the attacker can easily track the information or data about other Virtual machines [15].

4.1.5Virtual Networks:
Virtual Networks was one of the new features announced by Microsoft. Virtual machines are connected with virtual networks, which are shared by multiple tenants across the network. It gives attacker a way to get into the virtual network [16]. Most of the Virtual Machine Monitors use virtual network to communicate with each other directly [15].There can be possibility of spoofing and sniffing attacks in most of the virtualization platforms [14].

4.1.6Network and Internet connectivity issues:
IaaS-cloud providers supply on-demand from their large pools installed in data centers. For wide area connectivity, consumers can use either the Internet or carrier clouds dedicated to virtual private networks. Cloud Infrastructure is connected through internet and maintained at different locations so that it can be recovered and managed at the time of any unpredicted disasters. Usually, the local virtual machines are more prone to internal attacks compared to external attacks as the data is shared by locally connected VMs and the different malicious software can be run and installed by the administrator privileges. So, the IaaS environment is more vulnerable to internet or network attacks compared to any other cloud layer[31].

4.2 Security Issues in PaaS:
4.2.1Application development life cycle:
It is also a big challenge to secure a software application development because software developers face quite difficult to secure the application-taking place in cloud environment. The application needs to be upgraded by applying new patches or versions to keep them up-to-date and secure [16]. Developer should also aware of the legal issues of the data storage or the source code storage so that it could not be compromised [15].

4.2.2 Underlying Infrastructure security:
Cloud providers are responsible for underlying infrastructure security and the services running for applications [17]. So, the application developers have no privilege to access underlying infrastructure. SaaS and PaaS user can share the same applications because the software developed are delivered and used in SaaS while in PaaS, the development tool is used to develop and test the same application to be used by the SaaS users. So, there can be security concern about the user data and its storage [15].

4.2.3Third-party Relationship:
Third-party also plays a important role in PaaS as the some third-party components are required in web services like Mashups which helps in integrating more than one source component into a single unit [18]. PaaS users and developers also need to depend on the services provided by third-party and the web-based development tools.

4.3 Security Issues in SaaS:
4.3.1 Network Security:
In SaaS service model, different kind of data is flowing from client to cloud provider and also stored at the provider side. So, the data flowing over the internet needs to be secured to prevent the data hacking. Some strong encryption techniques are used to control using Transport layer Security (TLS) and Secure socket Layer (SSL) [5]. There are different types of attacks in network layer such as packet scanning, IP spoofing, Man in the Middle attacks (MITM) etc. There are strong risks that malicious attackers can exploit network security loopholes to sniff IP data packets.

4.3.2Data Accessibility:
Application or data accessing over the network makes the life easier for cloud users. But, it also opens a gateway for security issues. The specific policies must be defined by the organization to access the data to avoid any intrusion within the network. Multi-tenant deployment can expose the issue on the managing data access within the single cloud environment [5]. So, the provider must adhere with the policies set for such scenario.

4.3.3Availability:
Cloud vendor should ensure that users will have a regular access of data and their application services as well as hardware resources around the clock. Any malicious attack can make whole application or services unavailable to the users. Some proper action plan needs to be defined for unpredictable incidents in order to recover from the disaster and for up and running business. Amazan's EC2 faced a big blackout in 2011 due to some network defect in its one of the cloud zone [20]. Many of its clients like Reddit and Netflix had an adverse impact due to this network breakdown [19].

4.3.4 Data Integrity:
Data integrity is one of most critical element in terms of cloud security. It deals with unauthorized modification of data. In cloud computing, the transaction management security-using web services because HTTP doesn't provide proper support to transaction delivery. Data

encryption is a better option to secure data on different levels: Row level, table level and database level. Database level encryption comes under software level encryption, which is quite secure because user provides the key to encrypt, and decrypted using key. So, if the data is hacked even though it cannot be deciphered without availability of the key. Row level encryption is done with hardware level encryption [21].

4.3.5 Multi-tenancy:

In SaaS service model, multi-tenants share a same database. The tenant information can be at risk if any misconfigured software application source code or data leakage takes place. Based on specific security policies, the authentication should be given to the users so that only data will be modified or accessed into or from database for the particular tenant. The data of one client should be isolated from another client.

5. Current Cloud Security Solutions

A research on cloud security is constantly going all over the world. Major cloud providers are also involved in working on the security solutions. Cloud security Alliance (CSA) is actively involving all the cloud providers and other individual people to participate and come up with some sound solutions. Tsai et al. brings a fourth-tier framework specifically for web-based development environment, provides some security at some extent [22]. In [23], Ristenpartet. al. suggested that risks could be the attacks, so the cloud service providers should implement web-based co-residence check to control the attackers. Krugel et al. suggested the amount of packet-snifering output filtering for specific application services is a good approach to control security issues for specific services and network ports [24]. Kong et al. also suggested a good solution stated as "Partition-locked cache (PLcache) and random permutation cache (RPcache) to defeat cache-based side channel attacks" [25]. Raj et al. also suggested data security during processing using resource isolation method, by isolating the processor cache within the VMs and then isolating virtual cache from VMM cache [26]. The cloud security can also be enhanced by providing proper safeguard to operating systems and the virtual machines used for cloud network [27]. An introduction has mentioned about the cloud security by the association with trusted third-party to ensure the security in terms of communication, integrity and confidentiality [28]. Milne et al. point out a simple solution to just use private cloud [29]. Jyoti et al. suggest that the virtualization would be the best option to shield with the security, which provides less investment on hardware and multiple machines, are managed centrally with high-end security [30].

6. Conclusion

There are lots of advantages associated with the use of cloud computing. But, it also some security concerns which slow down the open acceptance of this technology. Cloud providers need to ensure the customer about the confidential data security. We have discussed on different security issues on services model level: IaaS, PaaS and SaaS. Network, shared resources, storage and virtualization are the main issues which are still immature and need to be looked ahead. We have also discussed current available solutions to overcome some common and major issues. We need to have better encryption techniques and integrated cloud security framework to make it more dynamic with scalability.

References

[1] Cloud Computing, http://www.cisco.com /web/solutions/trends/cloud/index.html
[2] Charlie Williams, Advantages of Cloud Computing, "http://www.2x.com/blog/2013/02/news/advantages-of-cloud-computing/"
[3] Priya Viswanathan, Cloud Computing – Is it really all that beneficial?, "http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm"
[4] Ms. Disha H. Parekh, Dr. R. Sridaran, " An Analysis of Security Challenges in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013
[5] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2010), doi: 10.1016/j.jnca.2010.07.006
[6] Zhifeng Xiao, Yang Xiao, "Security and Privacy in Cloud Computing", IEEE COMMUNICATIONS SURVEYS & TUTORIALS
[7] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, SugataSanyal, "A Survey on Security Issues in Cloud Computing"
[8] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing (2009), DOI 10.1109/SCC.2009.84
[9] Qi Zhang • Lu Cheng • Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", J Internet ServAppl (2010), vol. 1: pp. 7–18.
[10] R. L Grossman, "The Case for Cloud Computing, " IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
[11] Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270–4.
[12] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, and USA. IEEE Computer Society, Washington, DC, USA, pp 35–41.
[13] Garfunkel T, Rosenblum M (2005) when virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa.
[14] Reuben JS (2007) A survey on virtual machine Security Seminar on Network Security

http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final..pdf. Technical report, Helsinki University of Technology October 2007.
[15] An analysis of security issues for cloud computing, Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, Journal of Internet Services and Applications 2013, 4:5.
[16] Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42.
[17] Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25.
[18] Keene C (2009) The Keene View on Cloud Computing. Online available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. Accessed: 16-Jul-2011.
[19] Sanjay P. Ahuja and DeepaKomathukattil, A Survey of the State of Cloud Security, Network and Communication Technologies; Vol. 1, No. 2; 2012, ISSN 1927-064X.
[20] Thibodeau, P. (2011). Amazon outage sparks frustration, doubts about cloud. Retrieved fromhttp://www.computerworld.com/s/article/9216098.
[21] Hacigumus, H., Iyer, B., &Mehrotra, S. (2002). Providing database as a service. Data Engineering, 2002. Proceedings. 18th International Conference on, pp. 29-38, 07.
[22] Tsai W, Jin Z, Bai X. Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware. Beijing, China: ACM; 2009. p. 1–10.
[23] Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270–4.
[24] Krugel C, Toth T, Kirda E. Service specific anomaly detection for network intrusion detection. In: Proceedings of the 2002 ACM symposium on applied computing, 2002, p. 201–8.
[25] Kong J, O. Aciicmez, J.P. Siefert and H. Zhou, Deconstructing new cache designs for thwarting software cache-based side channel attacks, Proceedings of the 2nd ACM workshop on Computer security architectures, ACM, New York, USA, 2008, pp 25-34.
[26] Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009, p. 77–84.
[27] Santos N., K.P. Gummadi and R. Rodrigues, towards trusted cloud computing. Proceeding of the conference on hot topics in cloud computing, (Hot Cloud'09), Berkeley, CA, USA.
[28] Zissis D. and D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst., 2012, 28:583-592.
[29] MilneJ.Privatecloudprojectsdwarfpublicinitiatives, 2010, http://www.cbronline.com/news/private_cloud_projects_dwarf_public_initiatives_281009S [accessed:19June2010].
[30] Jyoti S., S. manish and G. Rupali, Virtualization as an engine to drive cloud computing security. Proceeding of the High Performance Architecture and Grid Computing, July 19-20, 2011, Chandigarh, India, pp: 62-66
[31] Mohd Rahul, Mohd Junedul Haque and Mohd Muntjir, Impact of Cloud Computing on IT Industry: A Review & Analysis. International Journal of Computer and Information Technology (ISSN: 2279–0764) Volume 01–Issue 02, November 2013

Author Profile

Mohd Muntjir received the B.Sc in Mathematics from Choudhary Charan Singh University Meerut U.P. in 2002 and M.C.A. degree in Computer Science from Hemawati Nandan Bahuguna University Srinagar Garhwal Uttarakhand in 2007. Since 2011, he is working with College of Computers and Information Technology Taif University Saudi Arabia. His research interests are DBMS, Cloud Computing, Sensor Networks, E-Commerce and Multimedia Technology.

Mohd Rahul received M.C.A. degree from Punjab Technical University Jalandhar, India and M.Tech (IT) degree from KSO University Karnataka, India. Since 2010, he is working with College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests are Cloud Computing, Computer Networks, E-Commerce and routing protocols etc.