Indian Journal of Science and Technology, *Vol 10(19), DOI: 10.17485/ijst/2017/v10i19/111016, May 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Key Security Issues and Existing Solutions in Cloud Computing Applications

E. Poornima[1], N. Kasiviswanath[2] and C. Shoba Bindu[3]

[1]G. Pulla Reddy Engineering College, Kurnool – 518007, Andhra Pradesh, India; poornimacse561@gmail.com
[2]Department of CSE, G. Pulla Reddy Engineering College, Kurnool – 518007, Andhra Pradesh, India; hodcse@gprec.ac.in
[3]Jawaharlal Nehru Technological University Anantapur, Anantapur – 515002, Andhra Pradesh, India; shobabindhu@gmail.com

Abstract

Cloud computing, otherwise known as on-demand computing model that enables access to computation and storage resources on the internet. However, consumers are apprehensive about adopting this computing model because it is still plagued by security issues. Security is still an un resolved problem in cloud applications.In this paper, we present the key issues of data security in the cloud computing technology , and are described in four areas: storage security, network security, data security and virtualization. We then discuss some frameworks for addressing the security issues. Issues related to standardization, multi-tenancy, and federation have also been addressed for extensive usage of cloud computing technology in various applications.

Keywords: Cloud Computing, Data Security, Multitenancy, Security

1. Introduction

Cloud computing is at present the most prominent buzzwords in the digital world because of its revolutionary model of computing as a utility. It provided increased scalability, flexibility, reliability,and decreased operational and support costs. The speed of establishment and the ease of scaling up or down on demand have changed the way computing and communication services are used while making them better, faster and cheaper[1].

The cloud computing model provides access to a shared pool of computing resources that the users can access through the internet[2,3]. Its two distinctive features include:

- the use of computation resources is under demand, and
- the dynamic and accurate assignment of computational resources are only done when they are strictly essential.

The fundamental rule of cloud computing is to transfer the computing services from the user remote computer to the network of interconnected and networked/virtualized computers[4] (Figure 1). Here, it is not required to purchase and maintain the necessary resources including network, server, storage, application, service, etc.; rather, they can be used from the cloud network. One of the studies conducted by National Institute of Standards and Technology [5,6] have defined cloud computing as "computing model that enables ubiquitous, convenient, and on-demand network access to shared configurable computing resources (e.g., servers, storage, networks, applications, and services).These resources can be rapidly provisioned and released with minimal management effort or service provider interaction"[7].

However, many potential cloud users are reluctant to adapt to cloud computing owing to the unaddressed cloud computing security issues[7,8]. Inability of the owner of the data to control the placement of data is one of the key security challenges faced in cloud. With the increased

*Author for correspondence

usage of the Internet-enabled mobile devices including smartphones and tablets, the amount of web-based threats also continue to rise in number thus leading to more complex situation[9]. Securing data is more critical in the Mobile Cloud Environment. Thus, it is required to effectively attend to the security issues in cloud environments to enable more superior and safe operation of clouds all over the industry[10]. Recently, many original research, comparative analysis and review papers have been published that dealt with cloud computing security issues[11,12,13]. However, enough clarity regarding the most pertinent issues in Cloud Computing security including the related threats, risks, vulnerabilities, requirements and solutions have not yet been achieved. In addition, the security aspects associated with the virtualization in the cloud is a foundational how ever its an inadequately researched area of research.

This paper offers a broad discussion on the various security issues. In addition, the paper also deals with identifying, classifying, organizing and quantifying the major cloud computing security concerns and presenting the related solutions. We also present a taxonomy of the security issues in cloud computing.

1.1 Service Models for Cloud Computing

NIST[5] have defined the following three main service models, four deployment model in cloud[14].

- Infrastructure as a Service (IaaS): In this layer, the cloud provider provides the user with both storage services as well as computing power including storage sevices or computation services,operating systems and the virtualization of hardware resources[15].
- Platform as a Service (PaaS): Here, the cloud provider provides a computing platform, tools, development environment and capability to help users build, test, and deploy web-based applications;
- Software as a Service (SaaS): Here, customer is given with a software or an application as services that can be accessed from any online device[16,17,18].

1.2 Cloud Computing Deployment Models

Cloud computing is applied for any of the following four deployment models namely 1)private cloud 2),public cloud, 3) hybrid cloud, and 4) community cloud.

1.2.1 Private Cloud

In this deployment model, the infrastructure is operated exclusively for an organization.

1.2.2 Public Cloud

In this model, the infrastructure is owned by the organization(cloud provider), and and rent the services or resources to the customers , public or a large industry group. However, this model is considered less safe and more exposed to risk compared to the other models, as its resources are located at an off-site location.

1.2.3 Hybrid Cloud

A hybrid cloud is a combination of 2 clouds.which can be a private cloud , community cloud , or public cloud[18,19] and are managed by a secure network. A hybrid cloud, as a collation of private and public clouds presents the dual benefits of each of these models thereby effectively overcoming their obstacles. This model aids in data and application portability and the infrastructure is placed at the on-premise and off-premise.

1.2.4 Community Cloud

Here the infrastructure supports a specific community and is shared by the several organizations. This cloud is controlled and shared by multiple organizations. It removes the security risks associated with the public clouds and the costs involved in the privacy

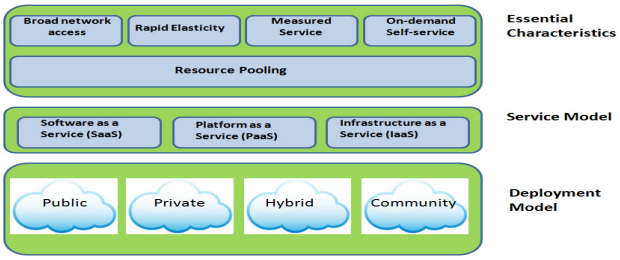

Figure 1. (a)Visual Working Definition of Cloud Computing. [31]

2. Cloud Computing Security Issues

Despite the benefits, there remain many open security issues because of multi-tenancy, outsourcing of application and data, and virtualization due to relocation to the clouds [20,21]. The information moves outside the user's security perimeter, which increases the users' overall security

risks. The IaaS model deals with providing basic security such as perimeter firewall, load balancing, etc. However, the applications that have moved into the cloud require greater levels of security provided by the host[10,22]. In thePaaS service model, the maintenanceof the incorruptibility of applications and proper enforcementof proper authentication checks during data transfer across the all networking channels is fundamental[22]. In SaaS applications are accessed using web browsers over the internet, so web browser security is important[22]. A few examples of security attacks in the cloud include (i) malware injection attack, (ii) wrapping attack, and (iii) DDoS attack. With regard to deployment models, more security than public and private clouds is seen in case of a hybrid cloud. In the case of private and public clouds, the former is more secure than the latter,which is considered as the least secure model[10,22]. Measuring the quality of security is difficult because the infrastructure should not be exposed.

Most of the security problems in cloud computing mainly stem from three broad reasons:

- loss of control of data,
- absence of trust (mechanisms), and
- multi-tenancy architecture.

All the above problems usually persist in the third-party management prototypes of the cloud. Apart from being associated with several privacy issues, public cloud also presents a number of security worries. , According to the recent survey, security was undeniably one of the top rated challenges of the cloud model[23]. This section of the paper deals with the high importance problems in cloud architectures. Although the private cloud guarantees security levels to a assured extent, the costs associated with this type of approach will be relatively high. Self-management clouds may in any case have security issues, but these issues are diversed to the above reasons.

2.1 Loss of Control of Data

Consumer's loss of control occurs owing to theplacement of data, applications, identity management of the users and resources with the provider The cutsomer directly depends on the cloud provider to guarantee factors like security and privacy for data, and availability of resources.

2.2 Lack of Trust (Mechanisms)

Trusting the third party means chance of getting in to danger. Although the trust relationships might not be so stronger at any instance in the cloud delivery chain, in order to ensure quick delivery of services[24]. A significant risk is introduced with the adoption of a cloud service owing to the globalized nature of the cloud infrastructure and non-transparency resulting due to the loss of control in transiting the sensitive data to other organizations. Organizations that are involved in contracting outsource business processes in the cloud may not be aware that the contractors may also sub-contract these processes. In such cases, the organizations may not know the identity of the sub-contracting providers in this contracting chain. In addition, the measures for the data protection may not be known in the contract chain. Furthermore, the data protection would result in weakening of trust at all levels from the customer to the providers. The 'on-demand' and 'pay-as-you-go' model are based on delicateconfidence relationship, with lax data security practices that may expose the data to third parties and makes it difficult inorder to check the deletions. With the aim of providing additional capacity at a shorter period, some new providers can then be appended to the chain without adequate verification regarding their identities,praices, reputations, and trust worthiness.

2.3 Multi-Tenancy

Generally the term Multi-tenancy refers to sharing of multiple resources and the services to execute software instances that serve multiple clients or tenants on a single machine (OWASP-10)[25]. ThePhysical resources in a cloud can be computing, networking, storage devices etc.. and the services are data storage, data management ,etc are supportedas well as it can be shared. The main driving force for cloud providers to have multi-tenancy is to cut down the costs by allowing the clients for sharing and reusing the resources among themselfs. In this environment, security is more dependent on the logical segregation of resources than the physical separation of the resources in aVM.

Some of the security issues arising due to multi-tenancy are as follows. (i) Inadequate logical security control. .This ensures that one tenant deliberately or inadvertently cannot interfere with the security (confidentiality, integrity, availability) of the other tenants. (ii) Malicious or ignorant tenants: A malicious or an ignorant tenant can reduce the security posture of other tenantsif the provider has weaker logical controls among the tenants. (iii) Shared services can develop into a single point of failure: If the cloud service provider has not constructed properly, they

can easily develop and results in misuse or abuse by the client.(iv) misconfigurations: When the multiple clients share this fundamental infrastructure, all the changes should be formed and must be tested. (v) Combined clients Data: The CSP stores themultiple clients data in the same database, makes use of same table-spaces, and uses same backup tapes to reduce the costs. This makes the data vulnerable and can lead to data destruction, which arises a security issue in the multi-tenancy, mainly if the data is stored in shared media.(vi) Performance Risks: The excess use of the service by a single tenant may effect the quality of service. (vii) XaaS Specific Risks are provided as follows:

SaaS: The application stack may be shared by the multiple clients or tenants. This indicates that data obtained from the multiple Users may be allocated in the same database, archived or backed-up . It is then moved through the common networking devices, and will handled by the application processes. This proves mainly focuses on the logical security to isolate different clients on a single VM.

PaaS: Since the platform layer is shared between the different tenants,the vulnerabilities in this layer will results in data leakageamong the clients.

IaaS: Security risks at Iaas includes cross-VM attacks and cross-network traffic listening. However, the co-residents may be faced with lower security posture [26].

3. Resolving Security Issues in the Cloud

In[12] has classified the security issues into seven main categories namely : 1) network security, 2) interfaces 3) data security 4) virtualization 5) governance 6) compliance and 7)legal issues. Each of the category have several securityissues, inturn classified into subdcategories highlighting the fundamental security issues identified in the base references[12,27] made a quantitative analysis of security aspect after analyzing more than 200 references.

However, data applications may still need to be in the cloud, and the consumers may not be able to manage taking back control. Trust mechanisms need to be improved by leveraging technology, policy, regulation, and contracts (for example, incorporating incentives). The higher trust in respect of the degree of isolation is essential. Multi-tenancy may be minimized by adopting private cloud. Virtual private cloud (VPC) is a system, and necessitates strong separation. While the providers of VPC argue that they present utmost isolation, since the consumers' data is not residing in the seperate servers and it is been stored along with the other user data. However, they are differentiated logically. In case of failure of the actual server, the consumers' files and apps stored are lost.

The presently available isolation facility within the clouds (i.e., virtualization) is not foolproof and can be easily attacked[28,29,30]. The problem becomes compounded when the same physical hardware hosts many tenants in the cloud. Therefore, the providers of cloud service should be certain about the information security on the cloud and resolve the risks to the acceptable level by using

- By using encryption scheme by which the shared storage areas protects all the data;
- By Specifying accurate access controls to avoid unauthorized access to the data; and
- Regular scheduled data backup's and storage of the backup media in secured.

This will require the establishment of information security system and trustworthiness between both the cloud providers and the universities[31].

4. Minimize Lack of Trust: Policy Language

It is a known fact that although the consumers have certain specific security needs, they do not have the authority to decide on the way they are handled. This means the consumers cannot state their requirements to the provider. In other words, the service level agreements (SLAs) are one-sided. These SLA's generally denote the high-level of policies set by the cloud provider (e.g., maintaing 98 percent). In particular, the communities of interest (COI) clouds encompass separate Security Policy essentials which must be fulfilled by the cloud provider owing to nature of COIs and their utilization. These requirements should be communicated to the providers so that they can ensure that the requirements are fulfilled. Thus, the cloud consumers and providers should be presented with a standard means for stating their security requirements and capabilities. This is made possible by devising a policy language that can be used to transferown policies and confidence, which is to be upheld by both the parties and used as an intra-cloud context to achieve the overall security aspects[32]. The cloud consumers need to devise a

way through which they can validate the given infrastructure and maintain the security mechanisms to satisfy the requirements as stated in the consumer's policy. Consider a case, where consumer's policy necessitates the isolation of virtual machines ,the CSP can devise a statement, stating that VM isolation is used for cache seperation . Additional assurances to consumers can be provided in the form of highly regarded, security features, assurance and risk assessment by certified third parties.

5. Minimize Loss of Control in the Cloud

5.1 Monitoring

The failure of the underlying components should follow the determination of, its effect so that the exact recovery measures meets.An application-related Run-time Monitoring and management tool can be used[32] in that situation. The applications placed in user computers,allowimg user to monitor and data flow. The outputs of the primitive services are directly issued to the application logic. If any data is found incompatibleamong the services is posed as a problem.The potential of the run-time monitoring and management tools should 1) aid the application user in determining the status of the cloud resources for running the application (across multiple clouds); 2) helpsthe users in determining the security issues in real-time and situational awareness 3) enable the application user to carry the tenant data or application (or a part of it) to the other Virtual Machine of the same cloud or of the different cloud 4) make the application user capable of changing the application logic on the fly; and 5) offer the cloud providers with communication capabilities.NimSoft and Hyperic are some cloud vendors[33] provides monitoring tools which are application specific functionalities. The further enhancement of these run time Monitoring tools might be carried out or might be combination with the other tools to provide certain degree of monitoring. Some how, it insists the tools for army purposes should also receive additional accreditation and Certificate procedures.

5.2 Utilizing different clouds

The services might be used by theconsumers from the different clouds via multi-cloud architecture[34], in which there are chances of increasing the risk, redundancy, as well as the chance of mission completion for several critical applications. However, the use of different clouds may lead to some particular issues such as policy incompatibility, data dependency between clouds, and knowing when to utilize the redundancy feature. Spreading the sensitive data across multiple clouds involves a lot of risk owing to the redundancy that could increase the risk of exposure.

5.3 Minimize Loss of Control: Access Control

Cloud computing has many layers in access control[35]. Based on the deployment model, the accesses are been controlled by the cloud provider or customer. Google Apps, is a provider and acts as a representative of SaaScloud,.In Google Apps, authentication and access policies are associated with its application and managed by the provider itself .On the other hand client or user has the resposibility of accessing their own documents through given interface. In the IaaS type approaches, the user holds the ability to build accounts on its VM and to create the access control lists for the services located on the VM.

The CSP manages the authentication and control access process irrespective of its deployment model.Few of the providers supports federated authentication, in which the client is able to manage its users, but they are responsible for the management of access control as well. This states that the user should have confidence on the service provider on all security related issues, data administration, and maintenance of the access control policies. This can turn out to be difficult with the involvement of the number of users from several organizations with of different access control policies. In case of theconsumer managed control access, the consumer is required to keep hold of the access control decision-making process as a means of control measure. This requires investing less trust on the provider (that means Packet Data Protocol (PDP) is in consumer's side). This model necessitates the client and the provider to have standard SLA and trust relationship to describethe users, resources. Furthermore, such approach should be equivalently secured as the traditional access control model. It is very much necessary that the data owner should have due involvement in all requests in such approaches. Therefore, this method should be avoided if traffic is an importantconcern. Hence, in many secure data outsourcing process, the users

is required to store keys or any certificates to the query side to involve the owner for every query to the database.

6. Minimize Multi-Tenancy in the Cloud

6.1 Local Host Security

Due to the lack of security in these terminal devices, untrust worthy services present in the cloud may attack the local networks. The local host machines used in the present computing environment includes desktop computers, laptops and mobile devices. In general, the cloud consumers are more concerned about the cloud provider's site security. Due to this, the consumers may forget to provide security to their machines. This lack of security can lead to compromising of the cloud and its resources for other users[36]. Mobile devices have higher threats. If a user depends on mobile for accessing cloud data this may increase the security threat as there is a possibility that the users may misplace or get their devices stolen. In addition, the potential attackers can easily enter the cloud system through handheld gadgets as the security mechanisms of tend to be insufficient as compared to the desktop computer.

Features like strong authentication mechanisms, tamper-resistance, and cryptographic functionality when there is requirement of traffic confidentiality should be embedded in a device that accesses cloud data. As a portion of detaining the security depends on the consumer, the provider may be required to stipulate its policy or SLA. In case of new cloud computing approaches in mobiles, the applications are required to lie in the cloud as compared to the smart phones that enable a greater sophisticated security mechanism.

Since the users use their local host machines to connect to the cloud, many of the secured cloud storing technologies ask for generating master keys (used for encrypting data, which are also known as session keys) that can be stored in the local machines used by the consumers. In consequence, if the local machine is attacked by a malicious service present in the cloud and these master keys are accessed, this causes data risk. In this case, the user's computer starts working like a zombie that can be easily accessed by the attackers to attack the stored data in the cloud. Malicious codes can be present in the computer of the user that can damage the provider-side resources, in turn affecting the provider as well as all its other consumers.

Hence, developing the new technologies can be enableb the war-fighters in the use of the handheld devices for gathering data to a command center. Hence , the major concern point rests at the robustness and durability of these devices both for cloud computing and general-purpose military use. Hence, for sensitive areas of memories, which is the site for storing keys, the memory curtaining techniques can be used. In addition, remote attestation or "Trusted Platform Module (TPM)" type requirements may be used for ensuring security of cloud computing.

7.Conclusion

Cloud computing presents an example of the standard mainframe client-server model, with scalable, universal and avaliability of resources. Both the traditional and new-era threats are involved in cloud. Security has become key issue in Cloud Computing environment,data security is to be managed for current technologies and research is to be carried out. Thus, the issues involved in ensuring the cloud data security in cloud computing, such as the lack of trust , the loss of control, and multi-tenancy problems needs to be identified,to make secure and reliable for cloud computing applications.This article reviews various security techniques for protecting the data in cloud and focused in improving data security, in providing a trustworthy healthy Cloud security environment for various applications.

8. References

1. GAP Report. Global Access Partners (GAP) Task Force on Cloud Computing. 2011.http://www.globalaccesspartners.org/Cloud-Computing-GAP-Task-Force-Report-May-2011.pdf
2. Buyya R, Broberg J, Goscinsky A. Cloud Computing: Principles and Paradigms. John Wiley and Sons;2011. Crossref
3. Sosinksy B. Cloud Computing Bible. John Wiley and Sons;2011.
4. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems.2009; 25(6):599–616 Crossref
5. NIST.http://csrc.nist.gov/groups/SNS/cloud-computing/2011.

6. NIST. http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html. 30th Dec 2012
7. Sangeetha T, Saranya M. Survey of security auditing issues in cloud computing. International Journal of Electrical Electronics and Computer Science Engineering. 2014;1(5): 33–36.
8. Gokulan V, Kalaikumaran T, Karthik S. Procuring data storage security in cloud environment by using two step secure protocol. International Journal of Software and hardware Reserach in Engineering.2014; 2 (4):102–7.
9. Donald A. Cecil, Oli S. Arul, Arockiam L. Mobile cloud security issues and challenges:A perspective. International Journal of Engineering and Innovative Technology.2013;3(1):401–6.
10. Jaffar Ali, Shareefa Rabiya N. Secure Cloud – A Survey. International Journal of Computer Science and Information Technologies.2014; 5 (4): 5447–49.
11. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013; 4(5): 2-13. Crossref
12. Gonzalez N, Miers C, Redígolo F, Simplício1 M, Carvalho T, Näslund M and Pourzandi M. A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications. 2012; 1(11):2–18.
13. Balasubramanian V, Mala T.A review on various data security issue in cloud computing environment and its solutions. ARPN Journal of Engineering and Applied Sciences. 2015;10(2):883–9.
14. Alotaibi MS. Utilization of cloud computing in library and information centers: A theoretical study. International Journal of Digital Library Services.2013; 3(4):83–93.
15. Fern´andez A, Peralta D, Herrera F, Ben´ýtez JM. An overview of e-learning in cloud computing. L. Uden et al. (Eds.):Workshop on LTEC. 2012; AISC. 173, pp. 35–46.
16. Kephart JO,Chess D M. The Vision of Autonomic Computing. Computer Magazine. January 2003 ed.
17. CSA. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance;2009.
18. David Hilley. Cloud computing: A taxonomy of platform and infrastructure-level offerings.CERCS Technical Report. Georgia Institute of Technology; PMid:19076107
19. NSAI Standards 2012. Adopting the Cloud - decision support for cloud computing. 4 April 2012.
20. Ristov S, Gusev M, Kostoska M. A new methodology for security evaluation in cloud computing., MIPRO. 2012 Proceedings of the 35th International Convention. 21-25 May 2012;p. 1484–89.
21. Chadha K, Bajpai A. Security aspects of cloud computing. International Journal of Computer Applications.2012; 40(8):43–47. Crossref
22. Kuyoro SO, Ibikunle F, Awodele O. Cloud computing security issues and challenges. International Journal of Computer Networks.2011;3 (5):
23. IDC. Enterprise Panel. September 2009. http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate
24. Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. 2nd IEEE International Conference on Cloud Computing Technology and Science. IEEE Computer Society.2010;. 693–702. Crossref
25. Open Web Application Security Project Cloud - 10 Project (OWASP-10); Multi Tenancy and Physical Security. https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security. Accessed 22nd May 2015.
26. Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my Cloud: Exploring Information Leakage in Third-Party Compute Clouds. Chicago, Illinois, USA;
27. CCS'09, November 9–13, 2009. Polash F, Abuhussein A, Shiva S. A survey of cloud computing taxonomies: rationale and overview. http://gtcs.cs.memphis.edu/pub/ICITST_Survey.pdf Accessed: 23rd May 2015
28. Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security Privacy.2011; 9(2):50–57. Crossref
29. Afoulki Z, Bousquet A, Rouzaud-Cornabas J. A security-aware scheduler for virtual machines on IAAS clouds. Report 2011.
30. Afoulki Z, Bousquet A, Rouzaud-Cornabas J, Toinard C. MAC protection of open Nebula cloud environment. In: International conference on high performance computing and simulation (HPCS).p. 85–90.
31. Shaikh FB, Haider S, Security Threats in Cloud Computing, 6th International Conference on Internet Technology and Secured Transactions. Abu Dhabi, United Arab Emirates:11-14 December 2011.
32. Jansen W, Grance T. National Institute of Standards and Technology (NIST) Guidelines on Security and Privacy in Public Cloud Computing. January 2011
33. G.Manoj Someswar, Smt.Hemalatha. Identification and implementation of suitable solutions to critical security issues in cloud computing. International Journal of Engineering Research and Development.November 2012; 4(7): 01–10.
34. Nikolay Grozev, Rajkumar Buyya. Inter-Cloud architectures and application brokering:taxonomy and survey. Softw.Pract.Exper. 2014; 44:369–390. Crossref
35. Md. Anwar Hossain Masud, MdRafiqul Islam, Jemal Abawajy. Security concerns and remedy in a cloud based e-learning system. In SecureComm 2013, LNICST 127. T. Zia et al. (Eds).
36. Sarvesh Kumar, Suraj Pal Singh, Ashwanee Kumar Singh, Jahangir Ali.Virtualization, The great thing and issues in cloud computing. International Journal of Current Engineering and Technology.2013; 3(2): 338–341.