ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Survey on Security Issues in Cloud Computing Environment

Rachna Jain[1], Gaurav Saxena[2], Anuj Madan[3], Saurabh Sharma[4], Nishant Pai[5]

Assistant Professor, Department of Computer Science, GGSIPU, BVCOE, Paschim Vihar, New Delhi, India[1]

UG Student, Department of Computer Science, GGSIPU, BVCOE, Paschim Vihar, New Delhi, India[2,3,4,5]

ABSTRACT: Cloud has introduced a new concept of provision of on-demand resource to services on internet. Cloud provides an attractive model while allowing the service providers to save cost. It allows users to free themselves of tasks of resource management i.e. most efficient use of resources. It also allows centralization of information and resources so that the users can access them from anywhere using the internet. Generally the resources used to provide services belong to a third party. As the users don't have to invest capital in such resources it decreases costs. Even though cloud model is lucrative, users have been hesitant in adopting it, the major reason being security concern regarding their private data. In this paper we discuss about various security concerns in cloud environment.

KEYWORDS: Cloud, IaaS, PaaS, SaaS, Security.

I. INTRODUCTION

Cloud computing has become a buzzword in the industry, gathering interest from individuals to large organisation. It provides an environment to users, allowing them to dynamically allocate and reallocate resources as required at any time instant. Cloud apart from providing easily-scalable architecture, also has become a common way to store and share files amongst the users. Due to its unique architecture, it faces some serious security issues, the most common being isolation and security of user data on the cloud. We first give a brief introduction about what is cloud computing and its various service and deployment models. Then we discuss about various security concerns in cloud environment followed by case study of security breaches known to have occurred. At the end we present literature survey on topics related cloud, security issues, safety of data in cloud.

II. CLOUD COMPUTING

"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*" [1]

Since its inception the concept of cloud has gathered interest not only of researchers but of large organisations as well. To end users cloud is a majorly data storage and sharing platform allowing them to access their files from anywhere. To professionals, cloud computing allows them to provide services on an architecture with the capability to dynamically manage various resources to handle varying amount of load. Cloud computing is soon becoming the most insidious delivery method for IT services across the public and private sectors. Benefits such as a wide range of tailor-made solutions and increased efficiency make cloud computing an attractive prospect.

Cloud computing has the following characteristics [2]:

1. *On demand self-services*: A consumer should be able to get computing services and network storage without human interaction.
2. *Broad network access*: Cloud capabilities are available over the network and accessed through standard mechanisms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

3. *Resource pooling*: The provider's resources are pooled together to serve multiple users and the resources are assigned and reassigned dynamically to fulfil consumer's demand.
4. *Rapid elasticity*: Cloud services can be rapidly and elastically provided, to quickly scale out and rapidly released to quickly scale in.
5. *Measured Service*: Cloud systems are capable of controlling and optimisation of resource usage through use of metering capabilities. Provide transparency by measuring, controlling and reporting of resource usage.

Depending on the purpose of setting up cloud and level of access to resources, there are 4 cloud deployment models: Public, Private, Hybrid and Community.

1. *Public Cloud:* Public Cloud provides infrastructure and computation resources over the Internet [3], which is provided some providers like Google, Amazon, and Microsoft. In public cloud, the infrastructure is owned by the service providers and the users are unaware and have no control over it. Public cloud are generally more effective than in-house cloud setups providing seamless on demand scalability. [4]
2. *Private Cloud:* In private cloud the computing environment is dedicated to one particular organisation [3]. Unlike public cloud it is not shared by any external entity, providing greater amount of security and control. Private cloud can be managed in the organisation itself, with the organisation itself paying for the physical resources used [4]. This arrangement gives the organisation complete control and configurability over resources. Private cloud can also be managed for an organisation by a third party and hosted within or outside of organisation's data centre [3].
3. *Community Cloud:* A community cloud falls between private and public cloud, wherein the infrastructure and computational services are shared between two or more organisations having similar requirements, privacy and security concerns [3].
4. *Hybrid Cloud:* Hybrid cloud is combination of the two or more clouds which may be private, public or community [3]. Hybrid cloud provides possibility to amalgamate private cloud service with public cloud, thus allowing management of any unexpected workload surges.

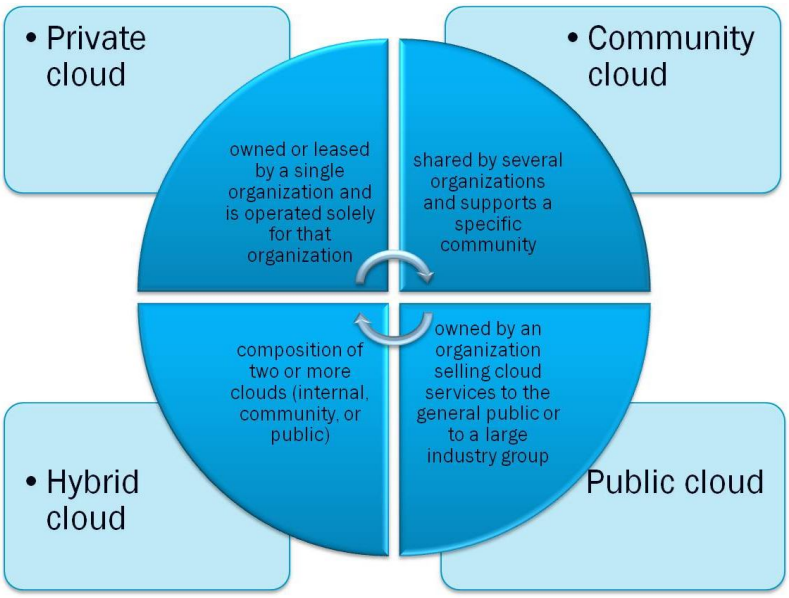

Fig. 1 Deployment Models [29]

Depending on how cloud based services are used, there are three cloud service models, Software as a Service, Platform as a Service and Infrastructure as a Service.

1. *Software as a Service:* Software as a Service (SaaS) provide applications deployed on cloud environment to end user. The user has no control over cloud's infrastructure or computational resources. The main purpose of SaaS is to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

reduce cost of software deployment, maintenance and operations. Office 365 is an example of SaaS provided by Microsoft. [5]

2. *Platform as a Service:* Platform-as-a-Service (PaaS) is targeted towards providing the environment and services for development of delivery of cloud based applications. PaaS provides an open or proprietary language to develop applications, set of services for communication with cloud. The cloud provides is responsible for task of management of resources allocated to application. [5] Microsoft Azure, Amazon AWS are examples of PaaS model.
3. *Infrastructure as a Service:* Infrastructure as a Service (IaaS) provides the basic infrastructure of servers, software and equipment upon which a platform to develop and execute applications can be developed. Its main purpose is to avoid purchase of hardware and software components and obtain them vie a service interface. [3]

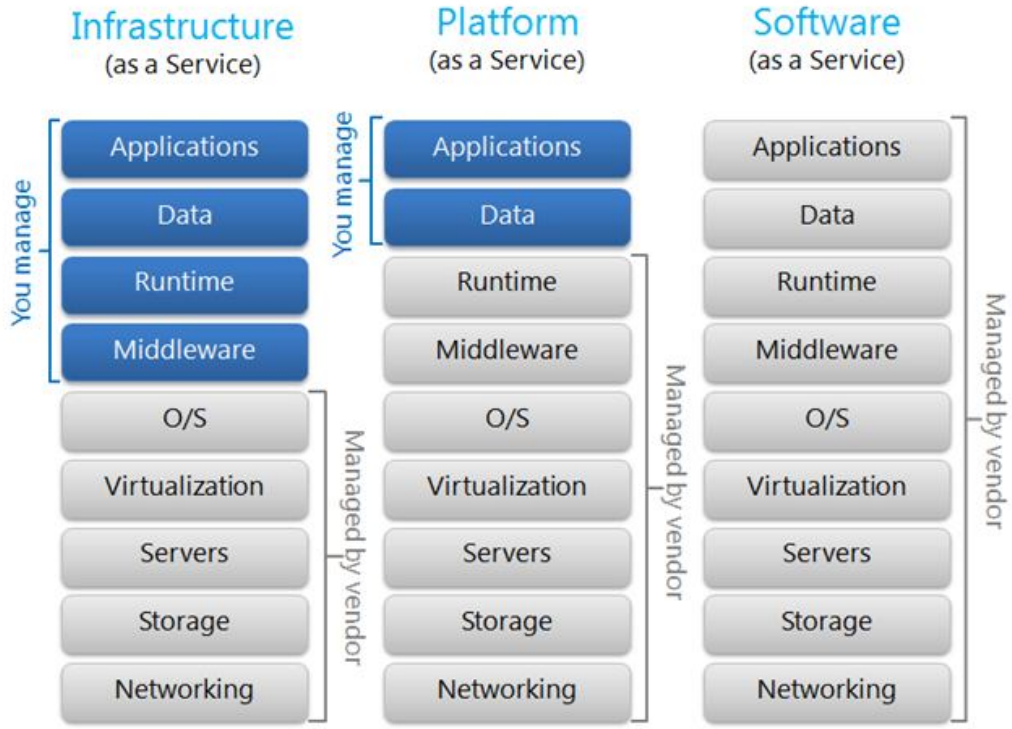

Fig. 2 Cloud Service Models [30]

III. SECURITY CONCERNS IN CLOUD ENVIRONMENT

Security of private and confidential data is the biggest concern amongst the user of cloud. Even after they save data on cloud, they might feel deprivation of control over it, the main concern being "who else might have access to their data". Sometimes, the service provider themselves outsource some services to scale them up or to save costs. Another issue is trust between users and service provider. Where users are most concerned about security and confidentiality of their data, service providers value the faithfulness and integrity of their users.

All the above concerns have restricted users from migrating or using cloud environment to provide their services. But the situation is improving as these issues are being addressed and people are adopting cloud environment which can be seen from Lierberman Software's 2014 Cloud Security Survey [6]:

- 79.65% of survey respondents (7.4% decrease from 2012) chose to keep their sensitive data on internal servers rather than on cloud.
- 33.21% (30.82% decrease from 2012) of respondents said the thought of government spying deters them from keeping data in cloud.
- 74.55% of respondents think that the cloud applications their users download cause security headaches.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Threats identified by "Cloud Security Alliance" (CSA) in cloud computing are [18]:

1. *Abuse and Nefarious Use of Cloud Computing. (*Applicable to IaaS and PaaS service models)

Many cloud provider allow easy registration to users with a valid credit card, with a certain level of anonymity. IaaS provides customer with illusion of unlimited computer resources. Spammers, malicious code authors and others have been able to utilise this anonymity to conduct their activities.

Recommendations made by CSA to prevent:

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks

2. *Insecure Application Programming Interfaces. (*Applicable to IaaS, PaaS and SaaS service models)

Cloud Computing service are provided through an APIs. The security of cloud services is dependent upon how secure these APIs are. Many third party vendors build application upon these APIs which further increases security consideration behind these APIs.

Recommendations made by CSA are:

- Analyse the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

3. *Malicious Insiders*

Applicable to IaaS, PaaS and SaaS service models.

The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Recommendations made by CSA:

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.

Determine security breach notification processes.

4. *Shared Technology Vulnerabilities. (*Applicable to IaaS service models)

IaaS service model follows multi-tenant architecture, wherein multiple users share infrastructure. Many of the components building the infrastructure do not provide isolation properties to multi-tenant architecture. A hypervisor is then used to overcome this gap, but even it has its own flaws. Therefore, to prevent users from impacting operation of other tenants on same cloud provider, strong compartmentalization should be used.

Recommendations by CSA:

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits

5. *Data Loss/Leakage.*

Deletion or alteration of record without backup, unlinking record from a larger context, loss of encoding key can result in loss of data. Due to characteristics of cloud the threat of data compromise increase in cloud.

Recommendations by CSA

- Implement strong API access control.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

- Encrypt and protect integrity of data in transit.
- Analyse data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers to wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

6. *Account or Service Hijacking. (*Applicable to IaaS, PaaS and SaaS service models)

Cloud adds another dimension to account or service hijacking. If an attacker gains access to a user's credentials, he can monitor user's activities and transaction, manipulate data, return false information, redirect user's client. The attacker can thus effectively use user's reputation to his own advantage.

Recommendations by CSA

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

7. *Unknown Risk Profile.*

Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture.

Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs.

Recommendations by CSA

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

Other cloud specific issues are [14] - [17]:

- isolation failure
- data interception
- insecure or incomplete data deletion
- lack of security perimeter
- larger attack surface
- Management interface compromise.

IV. CASE STUDIES

1. DropBox

Date: June 2011

Impact: Successful authentication using incorrect password.

A bug in Dropbox's authentication allowed people to login into user's dropbox account using invalid passwords.

According to Dropbox less than a 100 accounts were accessed using this vulnerability and all accounts were accessed by a single individual. As a response Dropbox sent E-mail to every users whose account was accessed using this vulnerability.

2. Microsoft Business Productivity Online Suite

Date: December 2010

Impact: A configuration error in Microsoft Business Productivity Online Suite left the users' contact information in offline Address Books exposed to other customers.

Offline Address Books Offline Address Book (OAB) is a downloaded copy of a Microsoft Outlook user's address list which allows the user access to email addresses when disconnected from Exchange Server. Microsoft stated that, the configuration error was fixed within two hours of discovering the error. [7]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

3. GoGrid
   - Date: 30 March 2011
   - Impact: Possible leakage of account information including payment card data of user to a third party user.

GoGrid stated in a mail to its customers, that an unauthorised third party user might have gained account information and possible payment card data. It also claimed that the method used to gain data had been identified and remediated, with the sole purpose behind the attack to gain free services from GoGrid. [8]

4. Apple iCloud
   - Date: 26 September 2014
   - Impact: Personal photographs leaked on the internet.

Apple denied that the leak was caused by any vulnerabilities in iCloud, and was caused due to a much targeted attack on user names, passwords and security questions.

Apple denies that its online systems had been breached. Apple said certain celebrity accounts were compromised by a much targeted attack on user names, passwords and security questions. A security researcher has reported to apple about possible vulnerability which allowed him to try more than 20,000 password combinations on Apple ID accounts, which is believed to be cause of data breach.

Apple suggests that users make sure they have a strong password and they enable two-step verification—a security feature that requires users to first type a password and then perform a second step, such as typing in a code. [9]

5. Sony's PlayStation Network
   - Date: April 20, 2011
   - Impact: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.

This is viewed as the worst gaming community data breach of all-time. Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers. Sony said that the PlayStation Network was compromised between the company said user account information for the PlayStation Network between April 17 and April 19. It is suspected that hackers took over PC of a system administrator, having access to sensitive information about Sony's customers. Access to the PC was obtained by sending the administrator an email with malicious software. Sony recommended users to place fraud alerts on their credit cards. [10]

6. Xbox Live
   - Date: March, 2014
   - Impact: No data loss was reported.

A 5 year old boy found vulnerability in Xbox live authentication system. It was found that typing in the wrong password and then typing spacebar, password verification could be bypassed through a backdoor [11]

7. Twitter Breach
   - Date: 1 February 2013
   - Impact: Date leak of usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users.

The company had detected an unusual access patterns leading to identification of unauthorized access attempts to Twitter user data. Bob Lord, Director of Information Security at Twitter stated that "This attack was not the work of amateurs, and we do not believe it was an isolated incident. The attackers were extremely sophisticated, and we believe other companies and organizations have also been recently similarly attacked. For that reason we felt that it was important to publicize this attack while we still gather information, and we are helping government and federal law enforcement in their effort to find and prosecute these attackers to make the Internet safer for all users." [12]

V. LITERATURE SURVEY

Seema Verma et al [19] in August, 2011 explained RSA public cryptosystem with its combined variants of Multiport RSA and Rebalanced RSA, i.e., RePower. Repower RSA provided the maximum decryption/signature generation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

performance of all the variants of RSA. But this performance is at the cost of very high encryption/ signature verification cost. She also explained DRSA to provide the semantic security to the system. The approach proposed in the paper gives better encryption performance at the cost of a small decrease in decryption side. It provides the semantic security to the system which RePower RSA does not. The scheme is proven to be better than RePower RSA as well as to DRSA.

Abdul Wahid Khan et al [20] in May-June 2012 published a literature survey in which he discussed data privacy/ protection issues and challenges in Cloud Computing. He explored the importance of the cloud computing along with the risks associated with the cloud computing procedure and process. He illustrated the data privacy problem in cloud computing environment. He defined different data protection models and techniques that show their contribution in cloud computing.

Priyanka Koduru et al [21] in January, 2013 applied RSA algorithm for providing data security in cloud environment. The performance of an algorithm on cloud network varies according to the type of the algorithm such as asymmetric, symmetric or hashing algorithms and also varies with the size of the input. In the proposed work only the authenticated and authorized user will be able to access the data, even if some unauthenticated user gets the access to data and if captures the data also, user cannot decrypt the data and get back the original data from it.

Parsi Kalpana et al [22] in September, 2012 gave the overview of data storage as well as security in cloud system in her report. She discussed various security attacks in cloud environment. She worked to provide integrity to the cloud storage area. In order to provide security RSA algorithm was used by author. The main goal is to securely store and manage the data so that only authorized users can have access over the data.

Anjana Chaudhary et al [23] in December, 2013 discussed the possible problems faced by present cloud. The main problem is data security issues in the cloud. Security of the Cloud relies on trusted computing and Cryptography. He proposed that only the authorized user can access the data. Even if unauthorized user gets the data, he can't decrypt it and get back the original data from it.

Tsai Wei-Tek et al [24] in 2010 situate this concept within the SOCCA and analyse how this architecture can help eliminate the lack of flexibility and isolation from other clouds. They discuss the theoretical possibilities and an experimental initial prototype developed by them.

Pallis George et al [25] in 2010 views cloud computing as a new "multidisciplinary research field" and seeks to engage in debates and dialogues by researchers and academicians on the same. He wishes to expand the theoretical framework surrounding this field of cloud computing and explore their full potential.

Shenai Sudhir et al [26] elaborate on the three service models of cloud computing, i.e. IaaS, PaaS and SaaS explicating the influence the cloud has on the internet. They however understand the business, technical and security challenges surrounding the cloud, and stress towards a need to address these concerns to optimize the user's experience.

Sarwar Azeem et al [27] address security concerns around cloud computing. They, in their paper, critically analyse gaps in "trust management" and the existing models. Through this dialogue, they encourage the CIA model (i.e. Confidentiality, Integrity and Applicability) to address the security concerns.

Vishal Garg et al [28] look at security concerns surrounding communication by analysing and finding the attack methods. They look at network security protocols in order to provide users and researchers with better encryption algorithms. It is important to understand vulnerabilities and develop algorithms to deal with them in case they get hacked.

VI. CONCLUSION

Cloud computing is a new concept which promises to provide easy to use and efficient service to its users. But still, there are security concerns the most common being about user's private data. This paper thus, introduced about the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

concept of cloud, various security issues related to it with the help of some real world examples and some of the many researches which have been done to improve security in cloud computing.

REFERENCES

[1] Peter Mell, Timothy Grance," The NIST Definition of Cloud Computing," NIST Special Publication 800-145
[2] http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud, 3 November 2014
[3] NIST Special Publication 800-144,"Guidelines on Security and Privacy in Cloud Computing," By Wayne Jansen Timothy Grance
[4] http://blog.appcore.com/blog/bid/167543/Types-of-Cloud-Computing-Private-Public-and-Hybrid-Clouds, 3 November 2014
[5] http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, 1 November 2014
[6] http://www.liebsoft.com/cloud-security-survey-2014/, 3 November 2014, 2 November 2014
[7]]http://www.dailytech.com/Microsoft+Lets+Users+Know+Their+Data+Was+Leaked+From+the+Cloud/article20482.htm, 3 November 2014, 30 October 2014
[8] http://cloudsecurity.org/blog/2011/03/30/gogrid-security-reach.html, 3 November 2014
[9] http://www.mirror.co.uk/news/technology-science/technology/apple-warned-icloud-vulnerability-months-432691, 3 November 2014
[10] http://in.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426, 29 October 2014
[11] thehackernews.com/2014/04/5-year-old-boy-discovers-microsoft-xbox.html, 3 November 2014
[12] https://blog.twitter.com/2013/keeping-our-users-secure, 3 November 2014
[13] http://techcrunch.com/2011/06/24/dropbox-breach-fewer-than-100-accounts-affected-but-one-person-actively-exploited-it/, 29 October 2014
[14] Krešimir Popovic, Željko Hocenski "Cloud computing security Issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija,Croatia
[15] Paul Wooley , Tyco Electronics ,"Identifying Cloud Computing Security Risks"
[16] V Venkateswara Rao, G. Suresh Kumar, Azam Khan, S SanthiPriya,"Threats and Remedies in Cloud
[17] A Survey on Cloud Computing Security, Challenges and Threats", Journal of Current Computer Science and Technology Vol. 1 Issue 4[2011]101-106
[18] "Top threats to Cloud Computing V1.0", Cloud Security Alliance, March 2010.
[19] Seema Verma Deepak Garg, "Improvement in RSA Cryptosystem" Journal of Advances in Information Technology, Volume 2, Number 3, August 2011
[20] Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem, "A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing", IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661 Volume 1, Issue 3 (May-June 2012)
[21] N.Padmaja, Priyanka Koduru, " Providing Data Security in Cloud Computing using public key cryptography", International Journal of Engineering Sciences Research-IJESR, ISSN: 2230-8504, e-ISSN-2230-8512 Volume 04, Special Issue , January 2013
[22] Parsi Kalpana and Sudha Singaraja, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Volume 1, Issue 4, September 2012
[23] Anjana Chaudhary and Ravinder Thakur, "A Review: Data Security Approach in Cloud computing by using RSA Algorithm", International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Volume 1, Issue 7 December 2013
[24] Tsai Wei-Tek, Sun Xin, Balasooriya Janaka, "Service-Oriented Cloud Computing Architecture", 2010 Seventh International Conference on Information Technology, 2010
[25] Pallis George, "Cloud Computing, The New Frontier of Internet Computing", IEEE Computer Society, 2010
[26] Shenai Sudhir, Aramudhan M, Monisha B, Suganya K, "Research Challenges in Cloud Computing", International Journal of Research in Engineering & Advanced Technology Volume 1, Issue 1, March 2013
[27] Sarwar Azeem, Khan Muhammed Naeem Ahmed, "A Review of Trust Aspects in Cloud Computing", International Journal of Cloud Computing and Services Science Volume 2. No.2, April 2013
[28] Garg Vishal, Rishu, "Improved Diffie-Hellman Algorithm for Network Security Enhancement", Int.J.Computer Technology & Applications, Volume 3(4), August 2012
[29] http://www.centre4cloud.nl/nl/kennis-ontwikkeling/definition-cloud-computing/deployment-models/
[30] https://www.spkaa.com/plm-in-the-cloud-computer-system-validation-in-fda-regulated-industries