International Journal of Scientific Research in Computer Science and Engineering
Review Paper Vol-1, Issue-5 ISSN: 2320-7639

A Comparative Study of Security Issues& Challenges of Cloud Computing

Mithilesh Mittal[1] Pradeep Sharma[2] and Pankaj Kumar Gehlot[3*]

[1,2,3*]*Department of Computer Science, Govt. Holkar Science College, Indore, India*

Available online at www.isroset.org

Received: 20 September 2013 Revised: 28 September 2013 Accepted: 17 October 2013 Published: 30 October 2013

***Abstract*—**Cloud Computing is rapidly changing the whole scenario of distributed system and it has given a fresh meaning to distributed system. Although Cloud Computing is delivering essential services and benefits such as low price services, on demand self-service, broad network access, large scale computation and highly availability of resources, but there are still some drawback behind services due to security issues and concerns. Cloud security Issues and challenges of Cloud Computing are identified in this paper through comparative study of three standard working organizations NIST(National Institute of Standards and Technology), CSA (Cloud Security Alliance) and ENISA (European Network and Information Security Agency).We briefly described all security issues and challenges of cloud computing identified by these working organization. After comparative study we observed a comparative based table which presents comparison of security issues and challenges of cloud computing.At the end of study we observed that all security issues are covered by all working organizations in term of security domain which are- 'strategic and policy issues' and 'technical issues' and 'legal issues'.

***Keywords*-**Cloud Computing; Cloud Service Models, Security Issues and challenges

I. INTRODUCTION

Cloud Computing is an on-demand self-service in which shared resources, information, software and other devices are provided according to the client's requirement at specific time. It is a term which is generally used in place of Internet. The whole Internet can be viewed as a Cloud. Many organizations, Alliances, working groups and researchers are working on Cloud Computing for enhancement of security aspects. All the consumers and Cloud Service Providers are concerning because of security, privacy and information integrity in all services of Cloud Computing. Security controls in cloud computing are not different from security controls in any IT environment. Security is a central concern for many cloud customers. Cloud customers have purchasing power on the basis of the reputation for confidentiality, integrity and resilience, and the security services offered by a cloud service provider, more than in traditional environments. This is a strong driver for cloud providers to improve their security practices and compete on security risks. Hence, security aspects of cloud computing are essential part for cloud service provider and cloud consumer.

II. CLOOUD COMPUTING:BACKGROUND STUDY

In the Cloud Computing the word 'Cloud' is used to describe kind of computing network because of the wordily used for describing network. There is not an official definition about what is Cloud Computing? For answering this question we can use NIST definition- The US National Institute of Standards and Technology (NIST) define Cloud Computing as "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" [1]. According to NIST Cloud services has five essential characteristics that demonstrate their relation to, and difference from, traditional computing approaches-On demand self-service, Broad Network access, Resource Pooling, Rapid Elasticity, and Measured Services. In [2] Rajkumar Buyya et.al proposed a definition of cloud computing-"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualised computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers".

A. Cloud Service Delivery Model

- Software as a Service (SaaS)
  Sometimes referred to as "On-demand software," is a software and its associated data are hosted centrally (typically in the (Internet) cloud) and are typically accessed by users using a thin client, normally using a web browser over the Internet [3].

- Platform as a Service (PaaS)
  It is the delivery of a computing platform and solution stack as a service. PaaS offering facilitate deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities. This provides all of the

Corresponding Author: *Pankaj Kumar Gehlot*

facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet [3].

- Infrastructure as a Service (IaaS)
  It delivers computer infrastructure (typically a platform virtualization environment) as a service, along with raw storage and networking. Rather than purchasing servers, software, data-center space, or network equipment, clients instead buy those resources as a fully outsourced service [3].

B. Cloud Deployment Model

Cloud Computing services and technology are deployed over different types of delivery models on their characteristics and purpose. Deployment models define where and how applications are deployed in a Cloud environment, such as publically with a global provider or private in local data centers. There are four main deployment model-Public Cloud Computing, Private Cloud Computing, Hybrid Cloud Computing, Community Cloud Computing [4].

- Public Cloud Computing- Public Clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability model of Cloud. In Public Cloud Computing the physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off-premises) [4].

- Private Cloud Computing- Private clouds are provided by an organization or their designated service provider and offer a single- tenant (dedicated) operating environment with all the benefits and functionality of elasticity and the accountability model of Cloud. In Private Cloud Computing the physical infrastructure may be owned by and physically located in the organization's data centers (On-premises) or that of a designated service provider (off-premises) with an extension of management and security control plans controlled by organization or designated service provider respectively [4].

- Hybrid Cloud Computing- Hybrid Clouds are a combination of Public and Private Cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offering and provide utilizing standard methodologies regardless of ownership or location [4].

- Community Cloud Computing- The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (example- mission, security requirements, and policy or compliance consideration). It may be managed by the organizations or by a third party and may be located on-premise or off-premises [4].

III. CLOUD COMPUTING SECURITY

Wikipedia [5] defines Cloud Computing Security as "Cloud Computing security (sometimes referred to simply as 'Cloud Security') is an evolving sub-domain of computer security, network security and more broadly information security. It refers to a broad set of policies, technologies and control deployed to protect data, applications and the associated infrastructure of Cloud Computing". Security is major concern in the cloud computing because cloud is repository of data and moving data to common location. Cloud computing is more attractive to attackers and more people are affected if an attack is successful [6]. The concern for security becomes more critical when the data is managed by third party service providers. As security issues and policies are not disclosed by CSPs to their clients at satisfactory level, clients are not aware of what security services CSPs are going to provide them. Cloud computing and web services run on a network structure so they are open to network type attack [7]. The Cloud Computing is new trend of distributed system and Internet is the medium between distributed environment and Clients. The Cloud Computing is running over the Internet and the security Issues in the Internet also effect cloud environment. Cloud Computing is not different from other traditional system. The traditional security problems such as security virus attack and hacking can also make concerns in cloud computing environment and can lead serious results. Malicious intruder and hacker may hack into cloud environment and misuse essential information stored in Cloud environment. In the Cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. The cloud consumers or clients do not know what the position of information; do not know which services are processing the data? The clients do not know what networks are transmitting the information? The clients don't ensure about data privacy operated by the Cloud Service Provider in a confidentiality way. Data integrity also issue of Cloud Computing system. Client must ensure about authorization and authentication process. So here we can say security is major concerns among other problems of Cloud computing.

IV. SECURITY ISSUES AND CHALLENGES

Study discusses about cloud computing platforms security issues and challenges provided by non-profit organizations which are industry representatives - Cloud Security Alliance (CSA), National Institute of Standard and Technology (NIST) and European Network and Information Security Agency (ENISA). In our study we use these three organizations and find out what security issues they have identified in their drafts and research journals.

A. Security Issues Identified by CSA

The CSA (Cloud Security Alliance) is one of the working organizations of Cloud Computing Security. The main motive

of this organization is to provide security assurance and education in the field of cloud computing area.It is a non-profit organization, initiated by industry representatives in November 2008. CSA supported by large number of IT companies, including Microsoft, Google, VMware, Amazon, IBM, Ericsson, etc. CSA published its first draft "Security Guidance for Critical Area Focus in Cloud Computing" on April 2009 which provides information about security issue in cloud computing platforms [8]. After that CSA published second draft "Security Guidance for Critical Area Focus in Cloud Computing v2.1" on December 2009 [9]. In our Study, we use the current version "Security Guidance for Critical Area Focus in Cloud Computing v3.0" of the draft. The guidance is divided into three domains. In this draft first domain named "Architectural Framework" gives brief information about cloud computing and its platform and reference model from the security perspective. The rest of the domains are divided into top two categories named governance and operation. The governance category discusses "strategic and policy issues of cloud computing platforms" and operation category describes technical perspective of security issues in cloud computing environment and their implementation within the architecture. Security issues identified by CSA [3] are listed below –

- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit
- Information Management and Data Security
- Portability and Interoperability
- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security as a Service

'Governance and Enterprise Risk Management' focuses on ability of an organization to govern and measure risks associated with cloud computing platforms. It Provides legal precedence for agreement breaches, ability of user organization to adequate assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues. It also recommends that security department should be included during Service Level Agreement and contractual obligations. 'Legal Issues: Contracts and Electronic Discovery' deals with legal issues associated with cloud computing platforms. A legal issue covers protection of the information and computer systems, security breach discloser laws, regulatory requirements, privacy requirements and international law to be followed by cloud providers.'Compliance and Audit'proves and maintains compliance when using cloud computing. This issue dealing with evaluating how clouds computing affects compliance with internal security policy as well as compliance requirements for cloud computing platforms, such as regulatory, legislative etc, and its impact on internal security policy. This issue includes some direction on providing compliance during an audit.'Information Management and Data Security' focuses on managing data that is placed in the cloud. It provides data manipulating such as creation, usage, sharing, storage, deletion, and archiving, It can be used to deal with the loss of physical control when moving data to the cloud. It identifies who is responsible for data confidentiality, integrity and availability. 'Portability and Interoperability' focuses on interoperability standards required among different cloud providers and also provides recommendation to be followed by both deployment and delivery models of cloud computing platforms. "Traditional Security, Business Continuity and Disaster Recovery" focuses how cloud computing affects the operational process and procedures currently used to implement security, business continuity, and disaster recovery. Traditional security functions of cloud platform are confidentiality, integrity, availability, backup, disaster recovery process for cloud storage. This section touches on helping people to identify how cloud computing may assist in diminishing certain security risks, or entails increases in other areas. 'Data Center Operations' provides information on how we can evaluate the provider's data center operation in order to select the best one for long term stability. This is primarily focused on helping users identify common data center characteristics that are fundamental to long-term stability. 'Incident Response Notification and Remediation' focuses proper and adequate detection, response, notification and remediation. It helps us to understand complexities, brought by cloud in current incident handling program. Further, it also addresses the necessary environment that is needed to be set up between both user and provider for proper incident handling and forensic. 'Application Security' secures application software that is running on or being developed in the cloud. Further, it also gives us information on security threats and vulnerabilities pertaining to cloud based delivery models (IaaS, PaaS and SaaS).'Encryption and Key Management 'identifies proper encryption usage and scalable key management. This section gives information on protecting access of data and resources. 'Identity and Access Management' focuses on importance of identity and access management in cloud environments. Further, it also focuses on federated identity and the problem faced by organization while extending its identity to cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based identity, Entitlement, and access management. 'Virtualization' discusses security issues related to system or hardware virtualization technology. Some of the items covered in this domain are hypervisor vulnerability, virtual machine isolation, risk associated with multi-tenancy.Finally, "Security as a Service" provides third party facility of security assurance, incident management,

compliance attestation and identity and access management. SeaaS is the delegation of detection, remediation, and governance of security infrastructure to a trusted third party with the proper tools and expertise. Users of this service gain the benefit of dedicated expertise and cutting edge technology in the fight to secure sensitive business operations.

B. Security Issues Identified by NIST

National Institute of Standards and Technology (NIST) is the another one working organization of cloud computing and other technologies. NIST government funded organization in the U.S. Department of Commerce, continuously assisting cloud computing platform users by identifying security-related vulnerabilities and issues in the cloud platform. Security issues discussed by NIST are specifically focused to public cloud vendors, as it states that organizations have more control of each layer of security when private cloud deployment model is used. Unlike other government funded organizations like, CSA and ENISA, NIST does not make any top level classification of security issues. However, each issue discussed by NIST can be linked with the sub-issue identified by other organizations. NIST published its draft "Guidance on Security and Privacy in Public Cloud Computing" on Jan. 2011 which provides information about security issue in public cloud computing platforms. Key security and privacy issues are identified by NIST [4] are listed below-

- Governance
- Compliance
- Trust
- Architectural
- Identity and Access Management
- Software Isolation
- Data Protection
- Availability
- Incident Response

'Governance'Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, testing, implementation and monitoring of deployed services of cloud computing. It extends organizational practices pertaining to the policies, procedures and standards used for application development and service provisioning in the cloud. It also raises an issue of information security risks. Enterprise risk is due to lack of control of services offered by cloud and it recommended using auditing tools and risking management program. 'Compliance'Involves conformance with an established specification, standard, regulation or law. This section discusses various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, and electronic discovery requirements. 'Trust'defines an organization relinquishes direct control over many aspects of security under the cloud computing paradigms. This section discusses various topic and issues of internal threats caused by Insider access, multi-tenancy, maintaining data ownership and intellectual property rights, risk management, gaining visibility and security control offered by CSP. 'Architecture' defines the underlying technologies the cloud provider uses to provision services, including the implications of the technical controls involved on the security and privacy of the system. This section discusses the issues pertaining to software systems which are utilized by cloud computing platform. Most of the issues discussed in this section are due to unique characteristics of cloud computing platforms which are completely different, compared to traditional data centers. The issues covered in this section are hypervisor security, virtual network protection, virtual machine images, client-side protection and server-side protection. 'Identity and Access Management' focuses on identity verification, authentication and access control mechanism. Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern in cloud computing, so here identity and access management function is adequate safeguards are in place to secure authentication and authorization. 'Software Isolation' defines virtualization and other software isolation techniques that the cloud service providers provide, and assess the risks involved. It warns about the threats associated with hypervisor complexity and multi-tenancy such as the attack vector. "Data Protection" Evaluates the suitability of the CSP's data management solutions for the organizational data concerned. Data stored in the cloud typically resides in a shared common cloud environment collected with data from other customers. Organizations moving sensitive and regulated data into the CSP' data centers, therefore, must account for the means by which access to the data is controlled and the data is kept secure. This section focuses on data isolation and data sanitization. "Availability" extents to which an organization's full set of computational resources is accessible and usable. It can be affected temporarily or permanently, and loss can be partially or completely. Denial of service attacks, equipment outages and natural disasters are some threats to availability. Finally, "Incident Response" section focus on reactive countermeasure for the attacks and threats in a cloud environment. It involves an organized method for dealing with the consequences of an attack against the security of a cloud system. CSP's role is vital in performing incident response activities, attack analysis, including verification, containment, data collection and preservation, problem remediation, and service restoration, and opposite to CSP, an organization's incident response strategy to address differences between the organizational computing environment and a cloud computing environment. Collaboration between the cloud service subscriber and cloud service provider in responding to an incident is essential to security and privacy in cloud computing platforms.

C. Security Issues Identified By ENISA

The European Network and Information Security Agency (ENISA) is another government funded organization of Europe aiming to provide better security and privacy functionality in cloud computing platform. ENISA published its first draft "Cloud Computing Benefit, Risk and Recommendation for Information Security" in November 2009. This document began with key benefits of security for cloud computing platforms. The rest of the document focuses security issues which are organized into three categories- Policy and organizational issue, Technical issues and Legal issues. Security issues categorized and identified by ENISA [10] are listed below –

Policy and organizational issue

- Lock-in
- Loss of governance
- Compliance challenges
- Loss of business reputation due to tenant activities
- Cloud service termination or failure
- Cloud provider acquisition

Technical issue

- Resource exhaustion
- Isolation failure
- Cloud provider malicious insider
- Management Interface compromise
- Intercepting data on transit
- Data leakage on up/download, intra cloud
- Insecure or ineffective deletion of data
- Distributed Denial of Service
- Economic Denial of Service
- Loss of encryption keys
- Undertaking malicious probes or scan
- Compromise service engine
- Conflict between customer hardening procedure and cloud environment

Legal Issue

- Subpoena and e- discovery
- Risk from change of jurisdiction
- Data Protection Risk
- Licensing risk

According to ENISA three main domains 'Policy and organizational issues', Technical issues, and legal issues are described. Each domain covers different risk and issues present in a cloud computing platform. Document describes each risk in five level which are probability level, impact level, reference to vulnerabilities, reference to the affected assets and level of risk. These five levels describe the nature of risk.

First level 'Policy and organizational issues' covers six different risks and issues which are briefly described here. 'Lock-in' discusses about data and service portability issue in terms of adoption of cloud service model SaaS, PaaS and IaaS. Afterwards, 'loss of governance' discusses portability issues and its impacts on organization assets, risks and vulnerabilities. It could have a potentially severe impact on the organization's strategy and therefore on the capacity to meet its mission and goals. It could lead to the impossibility with the security requirements, a lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service. 'Compliance challenges' discusses about affected assets like certification. Certification is essential for any organization either for competitive advantage or to meet industry standards or regulatory requirements. 'Loss of business reputation due to co-tenant activities' defines resource sharing that malicious activities carried out by on tenant may affect the reputation of another tenant. The impact can be deterioration in service delivery and data loss, as well as problems for the reputation of an organization. 'Cloud service termination or failure' the impact of this threat for the cloud consumer, could lead to a loss of service delivery performance and quality of service as well as a loss of investment.' Cloud provider acquisition 'impact could be damaging for crucial assets such as: the organization's reputation, customer trust and employee loyalty and experience.

The second domain of ENISA draft is 'Technical issues' which start with a list of threats present in a cloud computing platform. 'Resource exhaustion' defines level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections. 'Isolation failure' this class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure. The impact of failure can be a loss of valuable or sensitive data; reputation damage and service interrupt for cloud provider and their clients. 'Cloud provider malicious insider 'defines the malicious activities of an insider could potentially have an impact on the confidentiality, integrity and availability of all kind of data. 'Management interface compromise' is the customer management interface of public cloud providers are internet accessible and mediate access to larger sets of resources. This includes customer interfaces controlling a number of virtual machines and Cloud Provider interface controlling the operation of the overall cloud system. This risk may be mitigated by more investment in security by cloud service providers. 'Intercepting data on transit 'defines threat in data transfer. Data must be transferred in order to synchronize multiple distributed machine image, image distributed across multiple physical machine, between cloud infrastructure and remote web clients etc. Sniffing, spoofing, man-in-the attacks, side channel and replay attacks could be considered as threat sources. 'Data leakage on up/download, intra cloud' this is the same as the previous risk, but applies to the transfer of data between the cloud service provider and

cloud consumer. 'Insecure or ineffective deletion of data' defines data deletion risk, whenever a cloud provider is changed, resources are scaled down, physical hardware is reallocated etc. data may be available beyond the lifetime specified in the security policy hence security policy carry out the procedure of full data deletion is only possible by destroying a disk which also stores data from other clients. 'Distributed Denial of Service' and 'Economic Denial of Service 'are the scenarios in which a cloud customer's resources may be used by other parties in a malicious way that has an economic impact. 'Loss of encryption keys 'includes disclosure of secretes keys SSL, file encryption, customer private keys etc. or password to malicious parties. 'Undertaking malicious probes or scan' are indirect threats to the assets. They can be used to collect information in the context of a hacking attempt. The impact of this risk could be a loss of confidentiality, integrity and availability of service and data. 'Compromise service engine 'the service engine is developed and supported by cloud service provider vendors and the open source community in some case. It can be further customized by the cloud service provider. An attacker can compromise the service engine by hacking it from inside a virtual machine, the runtime environment and the application pool. 'Conflict between customer hardening procedure and cloud environment' it is a medium risk and the probability of this risk is low. Cloud service provider must set out a clear segregation of responsibilities that articulates the minimum actions customer must undertake. Cloud service provider should further articulate their isolation mechanisms and provide best practice guidelines to assist customers to secure their resources.

The third domain of ENISA draft is 'Legal issues 'which has four risk of cloud computing. The draft begins with 'Subpoena and e-discovery' which provide information on how to respond subpoena and electronic-discovery issues. 'Risk from changes of jurisdiction' customer data may be held in multiple jurisdictions, some of which may be high risk. If data centers are located in high-risk countries, those lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreement etc. could be raided by local authorities and data or system subject to enforced disclosure. 'Data protection risks' defines data protection risks for cloud customers and cloud service providers. Cloud customer will be the main person responsible for the processing of personal data, even when such processing is carried out by the cloud provider in its role of external processor. Failure to comply with data protection law may lead to administrative, criminal, and civil which vary from country to country, for the data controller. 'Licensing risks' focuses on customer license of cloud system. This risk affect service delivery of cloud system, this service should be real time service. This risk could be due to lack of completeness and transparency in terms of use of cloud computing system.

V. RESULTS AND DISSCUSSION

After study of all drafts our observation is that all working organization NIST, CSA and ENISA have identified various security issues and challenges in their draft. On the basis of observation we create a table which is given below-

TABLE I. COMPARATIVE BASED STUDY OF SECURITY ISSUES

Security Domain	Working organization of Cloud Computing		
	NIST	***CSA***	***ENISA***
Strategic and policy issues	✓	✓	✓
Technical issues	✓	✓	✓
Legal issues	✓	✓	✓

Table represents security domain and comparison among working organizations of cloud computing. We categorized three security domains in our comparison table which are 'strategic and policy issues', 'Technical issues' and 'Legal issues'. First domain 'Strategic and policy issues' includes governance policy, compliance and audit, service level agreement, trust, Cloud provider acquisition and other issues related to strategy and policy level negotiation between cloud consumer and cloud service provider. Second domain 'Technical issues' includes identity and access management, key management, incident response, malicious attacks, data loss or leakage, software isolation, data protection and other technical issues and Last domain 'Legal issues 'includes Subpoena and electronic discovery, Risk from change of jurisdiction, Data Protection Risk, Licensing risk etc. which are described in the draft.

These three category of security domain include all security issues and risks of cloud computing. After comparative study we observed that NIST, CSA and ENISA have categorized all security aspects in the draft. The study also found that NIST and CSA have not categorized their issues in different domain However, each issue discussed by NIST and CSA can be linked with the sub-issue identified by ENISA. So here we observed that NIST,CSA and ENISA identified different issues and challenges cover all area of security concerns in cloud computing, and all issues associated to three security domain.

VI. CONCLUSION

Security is essential aspect for providing a reliable environment and then enables the use of applications in the Cloud and for moving data and business processes to Cloud infrastructures. Our study observes that standard working organizations NIST, CSA and ENISA of cloud computing have identified all major concerns about cloud computing platform. Comparison table defines comparison among NIST, CSA and ENISA. After comparison we observed that NIST, CSA and ENISAidentified Strategic and policy issues', 'Technical issues' and 'Legal issues' in their draft. All

working organization identified same security domain in different sub-issues. Sub-issues are interlinked to these security domains. This paper provides comparative study of security issues identified by standard organizations.

REFERENCES

[1] P.Mell and T. Grance, "The NIST Definition of Cloud Computing" US National Institute of Science and Technology (NIST), 2011 http://csrc.nist.gov/publication/nistpubs/800-145/SP 800-145.pdf.

[2] Rajkumar Buyya, Chee Shin Yeo and Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities".

[3] Rajesh Piplode, Pradeep Sharma and Umesh Kumar Singh, "Study of Threats, Risk and Challenges in Cloud Computing", ISROSET-IJSRCSE Volume-01 , Issue-01, Page No : 26-30, Jan-Feb 2013

[4] Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, " Security Enhancement in Cloud Computing (CC)", ISROSET- IJSRCSE, Vol-1, Issue-1, pp(31-37), Jan-Feb 2013.

[5] Wikipedia- "Cloud Computing Security" http://en.wikipedia.org/wiki/cloud_computing_security.

[6] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vijendra Singh, "A Noval Open Security Framework For Cloud Computing" IJ-CLOSER Vol 1, No.2, june 2012, pp.45-52.

[7] Gurudatt Kulkarni , Jayant Gambhir, Tejswini Patil and Amruta Dongare "A Security Aspects in Cloud Computing" , 2012 IEEE.

[8] Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing" April. 2009; http://cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf.

[9] Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing v2.1" Dec. 2009; http://cloudsecurityalliance.org/guidance/csaguide.v2.0.pdf.

[10] D.Catteddn and G.Hogen, "Benefits, risk and recommendations for information security" ENISA (European Network and Information Security Agency), 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

