# A Survey On Security And Privacy In Cloud Computing

Kowsalyadevi Prakash
*Assistant professor*
*Dept. of computer science and engineering,*
*S.A.Engineering College, Chennai, India.*

**Abstract**

*Cloud computing is a growing area of concern in the IT security community. Basically, cloud computing is storing the data on someone else's computer and accessing it via a network. Many companies, such as Google.com, Amazon.com, Microsoft, Oracle/Sun, Canonical/Eucalyptus and many other vendors accelerate their paces in developing Cloud computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present a strong barrier for users to adapt into Cloud computing systems. This survey gives an overview regarding characteristics, security-architecture, and threats and existing solutions.*

## 1. Introduction

Cloud computing an emerging IT development, deployment and delivery model that enables real time delivery of a board range of IT products, services and solutions over the internet. Most of the data's are stored on local networks with servers that may be clustered and sharing storage. This approach has had time to be developed into stable architecture and provide decent redundancy when deployed right. A newer emerging technology-**cloud computing** has shown up demanding attention and quickly is changing the direction of the technology landscape (example: whether it is Google's

Unique and scalable Google File System, or Amazon's robust Amazon S3 cloud storage model). It is clear that cloud computing has arrived with much to be gleaned from[1].

Cloud is actually means that

"**C**ommon implies multi-tenancy, not Single or isolated tenancy
**L**ocation-independent
**O**nline
**U**tility implies pay for use pricing
**D**emand implies infinite, immediate, invisible scalability"

Here we do not confuse cloud computing with the term data center, as it typically sits on top of the latter. Viewing the cloud as logical rather than a physical, we can see it object describes it better in fig1.

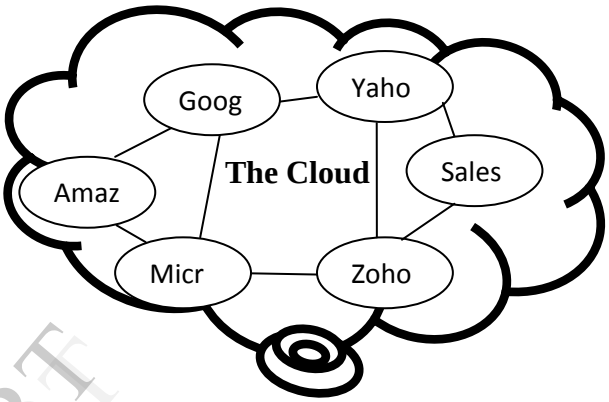


**FIG 1: Cloud computing conceptual diagram**

### 1.1 overview of cloud computing

Cloud computing is a model for enabling 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 promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud computing is not something that suddenly appeared overnight, in some forming it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications.

Many companies are delivering services from the cloud. Some notable examples as of 2010 include the following[2]:

• **Google** — has a private cloud that it uses for delivering many different services to its users, including email access, document applications, text translations, maps, web analytics, and much more.

• **Microsoft** — has Microsoft SharePoint® online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.

• **Salesforce.com** — runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.

### 1.2 Characteristics of Cloud Computing

It state that Cloud Computing allows business to increase IT capabilities on the fly and in real time i.e., Internet-enabled, without investing in new infrastructure, training new personnel or licensing new software, and as a pay-per-use service.

**Essential characteristics of Cloud Computing[3]:**

**1. On-demand self-service**

- It refers to the service provided by cloud computing vendors that enables the provision of cloud resources on demand whenever they are required.
- The user accesses cloud services through an online control panel.
- Example: The public providers like Amazon, Google, and Microsoft have this facet, smaller niche providers typically do not.

**2. Broad network access**

- It refers to resources hosted in a private cloud network that are available for access from a wide range of devices, such as tablets, PCs, Macs and smart phones.
- These resources are also accessible from a wide range of locations that offer online access
- These can include, Laptop, Desktop, Smartphone, Tablet device, and so on.

**3. Resource pooling**

- It means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly[2].
- Typically, user organizations of similar security levels or needs are grouped together on a particular community cloud offering all federal organizations, all pharmaceutical organizations, all general availability organizations
  - Examples: Storage, processing, memory, network bandwidth, and virtual machines.

**4. Rapid elasticity**

- The major characteristics that set cloud computing apart from traditional datacenter computing.
- Multiple tenants that share components of a shared resource pool (and in the case of a private cloud, all the tenants are part of a single corporate entity). Your tenants use the networking, compute and storage assets in the shared pool, and then return them to the pool when they no longer need those assets. They can also get more resources from the shared pool if and when they need to – but when they no longer need these additional resources, they return them to the pool. In a well architected cloud, the acquisition and release of assets from and to the shared pool would be automated, based on service demands and driven by an intelligence policy.

**5. Measured services or usage**

- It is simply called as ***Pay per use*** i.e., consumers are charged fees based on their usage of a combination of computing power, bandwidth use and/or storage
- Services can be scaled larger or smaller and use of a service is measured and customers are billed accordingly.
- Example: companies sell power to subscribers, telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service

**6. Multi Tenacity**

- It is a critical technology to allow one instance on application to serve multiple customers by sharing resources.

- It needs policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.
- The user might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

### 1.3 Services of Cloud Computing[3]

The Service model or Delivery model of cloud computing shown in fig 2 defines how cloud services are provided to consumers. It includes

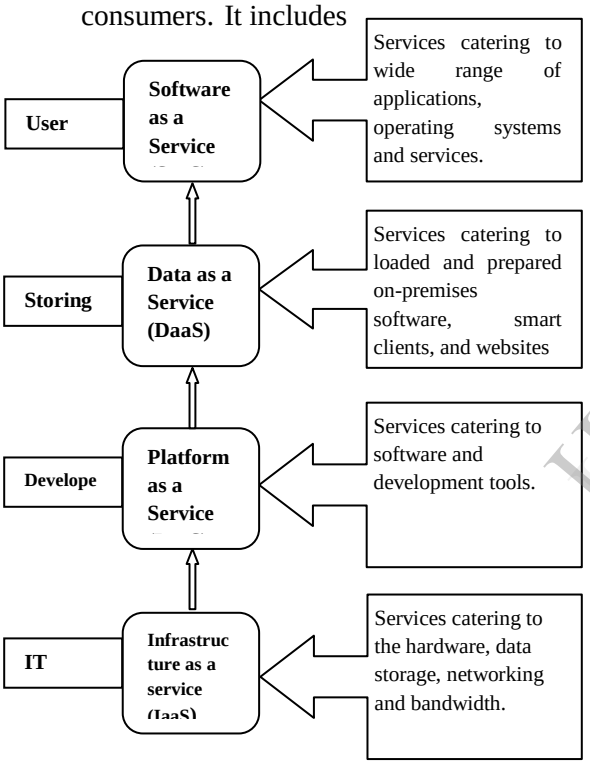


**FIG 2: Cloud Computing Services**

**a) Software as a Service (SaaS): (Application and Information clouds)**:

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser e.g., web-based email[3]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**b) Data as a Service (DaaS)**:

It is a cousin of software as a service. It is based on the concept that the product, data can be provided on demand to the costumer regardless of organizational separation of provider and consumer. It brings the idea that data quality can happen in a centralized place, cleansing and enriching data and offering it to different systems, applications or users. A common criticism is that when compared to traditional data delivery, the consumer is really renting the data,

**c) Platform as a Service (PaaS): (Development clouds)**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations

**d) Infrastructure as a Service (IaaS): (Infrastructure clouds)**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components[4] (e.g., host firewalls)

Here the service provider that offers customers storage or software services available via a private network or public network.

**2. Deployment Model:**

Cloud services can be deployed in three ways shown in table 1, depending upon the customer's requirements[4]:

**2.1 The Private Cloud:**

Private cloud or internal cloud or corporate cloud is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of customers.

A private cloud is designed to offer the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

**Tab 1: Cloud Service and Provider table**

| Cloud Services | providers |
|---|---|
| **SaaS** | **Salesforce.com, Gmail.com, WebEx, Google Docs, Acrobat.com** |
| **DaaS** | **IBM, HP, Microsoft, Google** |
| **PaaS** | **Amazon AWS, Google App Engine, IBM, NetSuite, Microsoft, Windows Azure, Force.com** |
| **IaaS** | **Rackspace, Go Grid, Sun Grid, SAVVIS, Terremark, World Wide, Windows Azure, Amazon AWS** |

**Advantages**

- Development, deployment and management of business applications at affordable expenses are extensively applied in Public clouds.
- Organizations can quickly convey highly scalable and reliable applications at more affordable expenses.

**Limitations**

- Regarding the security is so important in public clouds.

**2.2 The Public Cloud:**

Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.

**Advantages**

- Average server utilization are improved and also low-cost servers and hardware are permitted to use for providing higher capabilities; consequently costs are reduced that in other respects, a greater number of servers would require more.
- High levels of automation cause decrease in operations costs and managerial overheads

**Limitations**

- IT teams may have to spend in buying, creating and controlling the clouds independently in the organization.

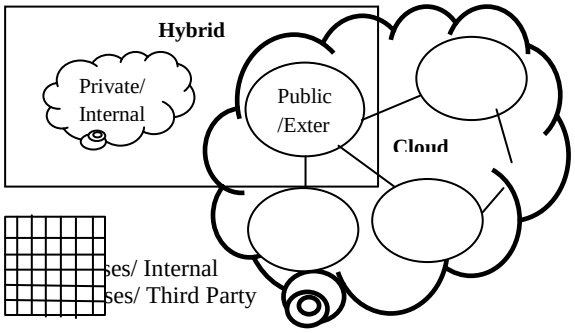


**Fig 3 Cloud Computing Types**

**2.3 Hybrid Cloud**

Combination of two or more clouds make the cloud infrastructure which remain as unique entities however normalized or characteristic technology that authorizes information and application portability attached them to each other[5] (e.g., cloud bursting for load-balancing between clouds). This is a composition of both private (internal) and public (external) cloud computing environments shown in fig 3. The hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

## 3. SECURITY ARCHITECTURE OF CLOUD COMPUTING

There are number of security concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. Here the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. Security has always been the main

issue for IT Executives when it comes to cloud adoption. However, cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. (ex., browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing)

Cloud security architecture is only effective if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:

**Deterrent Controls**

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

**Preventative Controls**

These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

**Corrective Controls**

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

**Detective Controls**

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

### 3.1 Feasibility of Cloud Computing

**Advantages of Cloud Computing**[6]

The following are some of the major advantages of cloud computing:

- **Virtualization:** Virtualization is defined as decoupling and separation of the business service from the infrastructure needed to run it.
- **Flexibility to choose vendor*:***
- **Elasticity:** Elastic nature of the infrastructure allows rapidly allocating and de-allocating massively scalable resources to business services on a demand basis.
- **Cost Reduction:** Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

Cloud computing benefits are

- Expand scalability
- Lower infrastructure costs
- Increase utilization
- Improve end-user productivity
- Improve reliability
- Increase security

**Disadvantages of Cloud Computing**

❖ **Security and privacy**[7]

To make their servers more secure, cloud service vendors have developed password protected accounts, security servers through which all data being transferred must pass and data encryption techniques. After all, the success of a cloud service depends on its reputation and any sign of a security breach would result in a loss of client and business.

❖ **Dependency-loss of control**

No influences on maintenance levels and fix frequency when using cloud services from a Cloud Service Providers. Backup, restore and disaster recovery are little insight in procedure. Migration is not easy.

❖ **Cost**

To make initial cloud offers more expensive.

❖ **Decreased flexibility**

This is only a temporary problem; they don't really offer the flexibility. The users might have to deal with the facts that their cloud server is difficult or impossible to upgrade without losing some data.

❖ **Knowledge**

More and deeper knowledge is required for implementing and managing (e.g. hardware, software, virtualization, deployment)

❖ **Integration**

Integration with equipment hosted in other data centers is difficult to achieve. (e.g. Bulk printers and local security)

## 4. Security Threats in Cloud Computing

### 4.1 Top Seven Security Threats[10]

Top seven security threats[10] to cloud computing discovered by "Cloud Security Alliance":

**1. Abuse and Nefarious Use of Cloud Computing**

Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines. Suggested remedies by the CSA to lessen this threat:

•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**

As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Suggested remedies by CSA to lessen this threat:

•Analyze 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.**

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.

Suggested remedies by CSA to lessen this threat[10]:

•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**

Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure[8] is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

Suggested remedies by CSA to lessen this threat:

•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.**

Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

Suggested remedies by CSA to lessen this threat[10]:

•Implement strong API access control.

•Encrypt and protect integrity of data in transit.

• Analyze data protection at both design and run time.

• Implement strong key generation[9], 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, Service & Traffic Hijacking.**

Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.

Suggested remedies by CSA to lessen this threat:

•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[10].

**7. Unknown Risk Profile.**

Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts – all things that should always be kept in mind.

Suggested remedies by CSA to lessen this threat:

•Disclosure of applicable logs and data.

•Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).

•Monitoring and alerting on necessary information.

## 5. Existing solutions for threats in cloud computing[11]

A cloud computing service is an operating model where business applications are delivered online rather than by a local server.

It allows:

- Access your system resources from anywhere at anytime
- Forget the headache of maintaining servers
- Commission desktops within minutes rather than days or weeks
- Upgrade the operating system and applications in a matter of minutes

Users work as if on their own desktop, with Microsoft Office, email and any specialist business applications in their start menu as if they are running locally. Consequently users can access their company desktop anytime, anywhere allowing flexible working and reduced IT costs.

**Mirage Image Management System**

The security and integrity of VM images are the foundation for the overall security of the cloud since many of them are designed to be shared by different and often unrelated users. This system addresses the issues related to secure management of the virtual-machine images that encapsulate each application of the cloud. Mirage Image Management System consists of 4 major components[11]:

- **Access Control**.

This framework regulates the sharing of VM images. Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions.

- **Image Transformation by Running Filters.**

Filters remove unwanted information from images at publishes and retrieval time. Filters at publish time can remove or hide sensitive information from the publisher's original image. Filters at retrieval time filters may be specified by the publisher or the retriever.

- **Provenance Tracking.**

The mechanism that tracks the derivation history of an image.

- **Image maintenance**.

Repository maintenance services, such as periodic virus scanning, that detect and fix vulnerabilities discovered after images are published.

**Client Based Privacy Manager**

Client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacy related benefits.

The main features of the privacy manager are:

• **Obfuscation**

This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and de-obfuscation is done using a key which is chosen by the user and not revealed to cloud service providers.

• **Preference Setting**

This is a method for allowing users to set their preferences about the handling of personal data that is stored in an un-obfuscated form within the cloud. This feature allows the user greater control over the usage of his data.

• **Data Access**

The Privacy Manager contains a module that allows users to access personal information in the cloud, in order to see what is being held about them and to check its accuracy. This is an auditing mechanism which will detect privacy violations once they have happened.

• **Feedback**

The Feedback module manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. This module could monitor personal data that is transferred from the platform.

• **Personae**

This feature allows the user to choose between multiple personae when interacting with cloud services.

**Transparent Cloud Protection System**

TCPS is a protection system for clouds aimed at transparently monitoring the integrity of cloud components. TCPS is intended to protect the integrity of guest Virtual Machines (VM) and of the distributed computing middleware by allowing the host to monitor guest VMs and infrastructure components. TCPS is a middleware whose core is located between the Kernel and the virtualization layer. By either actively or passively monitoring key kernel or cloud components TCPS can detect any possible modification to kernel data and code, thus guaranteeing that kernel and cloud middleware integrity has not been compromised and consequently no attacker has made its way into the system.

## 6. Conclusions

Several web service techniques are using cloud computing technique to provide their customers easy interface. Even though many systems overcome it has no standard framework. Cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. The cloud over the Internet provides the infrastructure required to supply services directly to customers. Security and privacy issues impose strong barrier for user's adoption of Cloud systems and Cloud services. The security and privacy concerns presented by an amount of Cloud Computing system providers in this paper. Nevertheless, those concerns are not adequate. More security strategies should be deployed in the Cloud environment to achieve the 5 goals (i.e. availability, confidentiality, data integrity, control and audit) as well as privacy acts should be changed to adapt a new relationship between users and providers in the Cloud literature. The prosperity in Cloud Computing literature is to be coming after that security and privacy issues resolved. Cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it.

## 7. Reference

1.Rohit Bhadauria, Rituparna Chaki,Nabendu Chaki, Sugata Sanyal, **"A Survey on Security Issues in Cloud Computing"**, 2009 IEEE International Conference on Services Computing, Bangalore, India

2.What is Cloud Computing? Retrieved April 6, 2011,available at: http://www.microsoft.com/business/engb/solutions/Pages/Cloud.aspx

3.Cloud Computing on Wikipedia, en.wikipedia.org/wiki/Cloudcomputing, 20 Dec 2009

4.Hero Modares, Rosli Salleh, Amirhosein Moravejosharieh, Hassan Keshavarz, Majid Talebi Shahgoli, **"A Survey on Cloud Computing Security"**, Archives Des Sciences, Vol.65, Issue.6, 2012. ISSN: 1661-464X

5.Mike Chung and John Hermans, "KPMG's 2010 Cloud Computing Survey"

6. Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, **"Security and Privacy in Cloud Computing: A Survey"**, 2010 Sixth International Conference on Semantics, Knowledge and Grids

7.Shilpashree Srinivasamurthy, David Q. Liu, **"Survey on Cloud Computing Security",** Department of Computer Science, Indiana University – Purdue University Fort Wayne, Fort Wayne, IN 46805

8.Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, "**A Survey on Cloud Computing Security, Challenges and Threats",** Rajnish Choubey et al. / International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. 3 Mar 2011

9. Poornima Nedunchezhian, Vidhyasree Venkatesh Moorthy, Palanikkumar Durai Thirunavukkarasu, **"A Survey on Challenges of Integrating Web Service in Cloud Computing",** International Journal of Computer Applications (0975 – 8887) Volume 44– No.1, April 2012

10. Top 7 threats to cloud computing DOI = www.netsecurity.org/secworld.php?id=8943

11. Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

12. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 978-0596802769. http://oreilly.com/catalog/9780596802776.

13. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 1-11.

14. J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853, 2008.

15. Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. White Paper. Information Systems Audit and Control Association, 2009.http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf