ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# An Assessment on Cloud Computing Data Security and Exploration

**V.Ashok Gajapathi Raju**
Asst.Professor,
Dept of CSE,
Aditya Institute of Technology and Management,
Tekkali, Srikakulam-India.

**G.Nagendra Kumar**
Asst.Professor,
Dept of CSE,
Aditya Institute of Technology and Management,
Tekkali, Srikakulam-India.

## Abstract:

Cloud computing is set of resources and provide services over the Internet. The services which are delivered from data centres that are located in the entire the world. General example of cloud services is Google apps provided by Google and Microsoft SharePoint. In cloud computing, IT-related capabilities are provided as services, accessible with minimal management effort and without requiring detailed knowledge of technologies. The rapid growth in cloud computing also increases severe security concerns. However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges and there are three critical challenges: regulatory, security and privacy issues in cloud computing-Security has always remained a constant issue for internet, when we are talking about security cloud really suffers.Cloud computing is surrounded by many security issues like securing data. Lack of security is the only hurdle in wide adoption of cloud computing.

## Keywords:

Interoperability, regulatory, security, privacy.

## INTRODUCTION:

Cloud computing has been developed by National Institute of Standards and Technology (NIST). Cloud computing is a model for on-demand network access to a shared pool of configurable computing resources i.e., networks, servers, storage, applications and services that can be hastily provisioned and released with minimal management effort or service provider interaction.

Cloud computing deliver the computing services over the Internet. Cloud provides the services to individuals and businesses to use software and hardware that are managed by third parties at remote locations. Online file storage, social networking sites, webmail, and online business applications are the examples of cloud services. This model allows access information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

There are four basic cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services.The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services. These four delivery models are:

(i) Private cloud in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.

(ii) Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service.

(iii)Community cloud in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

(iv) Hybrid cloud which is a composition of different cloud computing infrastructure (public,private or community). An example for hybrid cloud is the data stored in private cloud of a travel agencythat is manipulated by a program running in the public cloud.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## Characteristics:

The characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources 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.

## Service models:

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

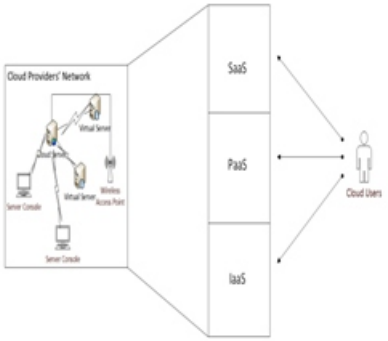


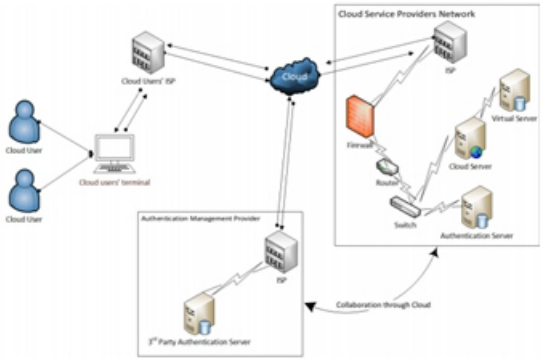

**Fig1. Cloud Service Hierarchy**

## Authentication in cloud:

The way to interact with devices, software, data and processes is drastically changed by Cloud computing but still some things never change and one thing that remains true across the old. New computing paradigms are the importance of authentication to confirm the identity of the user and/or system with which we're communicating.

Identity management and authentication form the basis for security whether in the cloud or on the local network. Managing identities has been enough of a challenge within the corporate network, and became more so as businesses formed federations for the purpose of sharing resources across organizational lines. Private, public and hybrid clouds are adding yet another layer of complexity. In a private cloud, to which users log on via a virtual private network, authentication can work effectively the same as on a local corporate network. Public clouds may be a different story, since it's all dependent on how the cloud vendor has implemented security.

Multi-factor authentication provides significantly more security but is being implemented slowly, even within local corporate networks, much less in the cloud. Biometric authentication has the potential to be the most secure form of single sign-on once the kinks are worked out, and solves some of the problems inherent in other forms of two-factor authentication. Users don't "forget" their fingerprints, lose them, or go off and leave them at home. And Hollywood fantasies aside, cases of the bad guys severing a finger or removing an eyeball to use it to gain unauthorized access are likely to be few and far between. However, a number of obstacles to adoption still exist, which include cost of biometric scanning equipment and users' fears of invasion of privacy.




## Deployment of cloud services:

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In a private cloud, the cloud infrastructure is operated solely for a specificorganization, and is managed by the organization or a third party. In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

## Cloud Computing Security And Privacy Issues:

This section addresses the core theme i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling,transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in intrusion detection systems (IDSs)


As shown inabove Figure, there are six specific areas of the cloud computing environment where equipment and software require substantial security attention These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication ofusers/ applications/ processes, (4) robust separation between data belonging to different customers, (5)cloud legal and regulatory issues, and (6) incident response.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group's White Paper, 2010). These self-encrypting build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.Encryption is the best option for securing data in transit as well. In addition, authentication andintegrity protection mechanisms ensure that data only goes where the customer wants it to go and it is notmodified in transit.

Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard,there are additional challenges associated with this. Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits.

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing andimplementing security control in a privately owned cloud.

- The treats against information assets residing in cloud computing environments.

- The types of attackers and their capability of attacking the cloud.

- The security risks associated with the cloud, and where relevant considerations of attacks and countermeasures.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- Emerging cloud security risks.

## Potential privacy risks:

While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate. Concerns have been raised by many that cloud computing may lead to "function creep" — uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. Given how inexpensive it is to keep data, there is little incentive to remove the information from the cloud and more reasons to find other things to do with it.

Security issues, the need to segregate data when dealing with providers that serve multiple customers, potential secondary uses of the data—these are areas that organizations should keep in mind when considering a cloud provider and when negotiating contracts or reviewing terms of service with a cloud provider. Given that the organization transferring this information to the provider is ultimately accountable for its protection, it needs to ensure that the personal information is appropriate handled.Privacy is not a barrier but it must be taken into considerationThe Personal Information Protection and Electronic Documents Act (PIPEDA) does not prevent an organization from transferring personal information to an organization in another jurisdiction for processing.

However, PIPEDA establishes rules governing those transfers — particularly with respect to obtaining consent for the collection, use and disclosure of personal information, securing the data, and ensuring accountability for the information and transparency in terms ofpractices. For more information on the views of the Office of the Privacy Commissioner of Canada with respect tooutsourcing of personal data processing across borders, please see our Guidelines for Processing Personal Data Across Borders. These considerations apply whether moving data in the cloud or otherwise.It is important to note that many non-Canadian based cloud providers may also be subject to PIPEDA. To the extent that a cloud provider has a real and substantial connection to Canada, and collects, uses or discloses personal information in the course of a commercial activity, the provider is expected to protect personal information, in keeping with PIPEDA.

## Securing the Multi-Tenant Environment:

## Hypervisor-Based Segmentation:

Virtualization is quite often the platform that underpins IaaS offerings. Software, such as VMware VSphere, CitrixXenServer, and Microsoft Hyper-V, provides the means of turning a single piece of hardware into a physical host formany VMs. These virtual machines are the databases, file servers, application servers, and Web servers that comprisethe typical physical network, and enable the traffic that makes commerce and communication over the Internet possible. They are also the servers offered to customers of IaaS for storing their data or running their web-based businesses. At its core, the virtualization platform includes a very specialized and optimized OS called the hypervisor,which in part serves to map traffic from VMs to the underlying VM host hardware so that it can make its way through the data center and out to the Internet and vice versa. The majority of security concerns in the virtualized infrastructure relate to the co-residency of machines owned by different customers.

This places machines in a privileged position relative to one another. And this can elevate the risk for many types of breaches such as unauthorized connection monitoring, unmonitored application login attempts, malware propagation, and various "man in the middle" attacks.VM segmentation and isolation is also an absolute requirement for VMs containing regulation and compliance intensedata like employee details, customer information, etc. Most regulatory mandates such as Payment Card IndustryData Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA ), Sarbanes-Oxley Act(SOX), and Gramm Leach Bliley Act (GLBA) require that access be limited to a business' need to know, and that controlpolicies be set in place to enforce blocking of unwarranted access. Since the hypervisor intercepts all traffic betweenVMs and VM hosts, it is the natural place to introduce segmentation for the resources of IaaS tenants where VMs mightbe housed within the same VM host or VM host cluster.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## CONCLUSION:

Cloud providers need to safeguard the privacy andsecurity of personal data that they hold on behalf of organisations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is notcompromised. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloudbasedservices – without trust, customers will be reluctant to use cloud-based services. Privacy protection builds trust between service providers and users: accountability and privacy by design provide mechanisms to achieve the desired end effects and create this trust. This management can span a number of layers: policy, process, legal and technological. It is universally accepted as best practice that such mechanisms should be built in as early as possible into a system's lifecycle.

We are currently carrying out research on ways to improve the protection of private data and thereby enable further deployment of cloud technologies; these mechanisms include identity management, sticky policies and data obfuscation. By these means users and citizens can be provided with reassurance that their personal data will be protected, and cloud deployments can be made compliant with regulations, even within countries where such regulation is relatively strict. The advantages of cloud computing – its ability to scale rapidly (through subcontractors), store data remotely (in unknownplaces), and share services in a dynamic environment –can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. In this paper we have assessed some of the key issues involved, and set out the basis of some approaches that we believe will be a step forward in addressing this situation.

## REFERENCES:

1."Understanding Cloud Computing Vulnerabilities," by B. Grobauer, T. Walloschek and E. Stöcker, IEEESecurity and Privacy, vol. 99, 2010.

2. "An analysis of security issues for cloud computing" Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1

3."Cloud Computing-A Practical Approach" byVelte, Tata McGraw-Hill Edition (ISBN-13:978-0-07-068351-8

4."Addressing cloud computing security issues Dimitrios"Zissis, DimitriosLekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, GreeceArticlehistory:Received 14 May 2010 Received in revised form 11 December 2010 Accepted 13 December 2010 Available online 22 December 2010

5. "A survey on security issues in service delivery models of cloud computing" S. Subashini, V.KavithaAnna University Tirunelveli, Tirunelveli, TN 627007, IndiaArticle history: Received 3 March 2010 Received in revised form11 July 2010Accepted 11 July 2010

6. "An Overview and Study of Security Issues & Challenges inCloudComputing"by Rajesh Piplode* Umesh Kumar SinghDepartment of Computer Science Institute Of Computer Science Govt. Holkar Science College Indore-India Vikram University Ujjain-India

7.http://www.conres.com/cloud-computing-deployment-models