



## Performance Analysis of Web Based Applications by Using Cloud Computing

Sadhana Rana

Assistant Professor Amrapali Institute of Technology & Sciences  
Haldwani, Nainital, Uttarakhand, India

---

**Abstract:** *Cloud computing is a new way of delivering computing resources, not a new technology. Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. Since we are in a time of belt-tightening, this new economic model for computing has found fertile ground and is seeing massive global investment. Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine. Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable. This paper explains, based on concrete scenarios, what cloud computing means for web applications, network and information security, data protection and privacy. We look at the security benefits of cloud computing and its risks. We cover the technical, policy and legal implications. Most importantly, we make concrete recommendations on how to address the risks and maximise the benefits.*

**Keywords:** *RAT, Web risk, cloud computing analysis*

---

### I. INTRODUCTION

Cloud computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The risks and benefits associated with each model will differ and so will the key considerations in contracting for this type of service. The following sections attempt to make the distinction when the risks or benefits apply differently to different cloud models.

**Software as a service (SaaS):** is software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc).

**Platform as a service (PaaS):** allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine.

**Infrastructure as service (IaaS):** provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.

### II. RECOMMENDATIONS

#### Assurance for Cloud Customers

Cloud customers need assurance that providers are following sound security practices in mitigating the risks facing both the customer and the provider (e.g., DDoS attacks). They need this in order to make sound business decisions and to maintain or obtain security certifications. An early symptom of this need for assurance is that many cloud providers are swamped with requests for audits. For this reason, we have expressed many of the report's recommendations as a standard list of questions which can be used to provide or obtain assurance.

Documents based on the check-list should provide a means for customers to:

1. Assess the risk of adopting cloud services;
2. Compare different cloud provider offerings;
3. Obtain assurance from selected cloud providers;
4. Reduce the assurance burden on cloud providers.

The security check-list covers all aspects of security requirements including legal issues, physical security, policy issues and technical issues

### III. LEGAL RECOMMENDATIONS

Most legal issues involved in cloud computing will currently be resolved during contract evaluation (ie, when making comparisons between different providers) or negotiations. The more common case in cloud computing will be selecting between different contracts on offer in the market (contract evaluation) as opposed to contract negotiations. However, opportunities may exist for prospective customers of cloud services to choose providers whose contracts are negotiable. Unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement entities. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the parties' use of the cloud, or responsibilities for infrastructure.

### IV. SECURITY BENEFITS

**Security and the benefits of scale:** put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, etc. Other benefits of scale include: multiple locations, edge networks (content delivered or processed closer to its destination), timeliness of response, to incidents, threat management.

**Security as a market differentiator:** security is a priority concern for many cloud customers; many of them will make buying choices on the basis of the reputation for confidentiality, integrity and resilience of, and the security services offered by, a provider. This is a strong driver for cloud providers to improve security practices.

### V. STANDARDIZED INTERFACES FOR MANAGED

**Security services:** large cloud providers can offer a standardized, open interface to managed security services providers. This creates a more open and readily available market for security services.

**Rapid, smart scaling of resources:** the ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (e.g., against DDoS attacks) has obvious advantages for resilience.

**Audit and evidence-gathering:** cloud computing (when using virtualisation) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down-time for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance.

**More timely, effective and efficient updates and defaults:** default virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes; IaaS cloud service APIs also allow snapshots of virtual infrastructure to be taken regularly and compared with a baseline. Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model.

**Benefits of resource concentration:** Although the concentration of resources undoubtedly has disadvantages for security [see Risks], it has the obvious advantage of cheaper physical parameterization and physical access control (per unit resource) and the easier and cheaper application of many security-related processes.

### VI. SECURITY RISKS

The following points should be noted in relation to the descriptions of risk below:

- Risk should always be understood in relation to overall business opportunity and appetite for risk sometimes risk is compensated by opportunity.
- Cloud services are not only about convenient storage, accessible by multiple devices, but include important benefits such as more convenient communication and instant multi-point collaboration. Therefore, a comparative analysis needs to compare not only the risks of storing data in different places (on premises v the cloud) but also the risks when on premises-data stored on premises – e.g. a spreadsheet - is emailed to other persons for their contributions, against the security issues of a spreadsheet stored in the cloud and open to collaboration between those persons. Therefore, the risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models.
- The level of risk will in many cases vary significantly with the type of cloud architecture being considered.
- It is possible for the cloud customer to transfer risk to the cloud provider and the risks should be considered against the cost benefit received from the services. However *not all risks can be transferred*: if a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage.
- The risk analysis in this paper applies to cloud technology. It does not apply to any specific cloud computing offering or company. This paper is not meant to replace a project-specific organisational risk assessment.
- The level of risks is expressed from the perspective of the cloud customer. Where the cloud provider point of view is considered, this is explicitly stated.

The most important classes of cloud-specific risks are:

**Data protection:** cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

**Insecure or incomplete data deletion:** when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

**Isolation failure:** multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g., against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

**Malicious insider:** while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service provider

## VII. THE BENEFITS OF CLOUD COMPUTING:

As cloud computing begins to take hold, several major benefits have become evident:

**i. Costs:** The cloud promises to reduce the cost of acquiring, delivering, and maintaining computing power, a benefit of particular importance in times of fiscal uncertainty. By enabling agencies to purchase only the computing services needed, instead of investing in complex and expensive IT infrastructures, agencies can drive down the costs of developing, testing, and maintaining new and existing systems.

**ii. Access:** The cloud promises universal access to high-powered computing and storage resources for anyone with a network access device. By providing such capabilities, cloud computing helps to facilitate telework initiatives, as well as bolster an agency's continuity of operations (COOP) demands.

**iii. Scalability and Capacity:** The cloud is an always-on computing resource that enables users to tailor consumption to their specific needs. Infinitely scalable, cloud computing allows IT infrastructures to be expanded efficiently and expediently without the necessity of making major capital investments. Capacity can be added as resources are needed and completed in a very short period of time. Thus, agencies can avoid the latency, expense, and risk of purchasing hardware and software that takes up data center space and can reduce the traditional time required to scale up an application in support of the mission. Cloud computing allows agencies to easily move in the other direction as well, removing capacity, and thus expenses, as needed.

**iv. Resource Maximization:** Cloud computing eases the burden on IT resources already stretched thin, particularly important for agencies facing shortages of qualified IT professionals. The cloud presents an environment where users can develop software-based services that enhances collaboration and fosters greater information sharing, not only within the agency, but also among other government and private entities.

**vi. Customization:** Cloud computing offers a platform of tremendous potential for creating and amending applications to address a diversity of tasks and challenges. Its inherent agility means that specific processes can be easily altered to meet shifting agency needs, since those processes are typically changeable by making a configuration change, and not by driving redevelopment from the back-end systems (Heyward and Rayport, 2009).

## VIII. CONCLUSION

The conclusion of this paper is that the cloud's economies of scale and flexibility are both a friend and from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective. This paper allows an informed assessment of the security risks and benefits of using cloud computing - providing security guidance for potential and existing users of cloud computing.

## REFERENCES

- [1] <http://www.cloudsecurityalliance.org/topthreats>
- [2] <http://www.malwaredomainlist.com>
- [3] [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Outlook/Udo%20Helmbrecht\\_ENISA\\_Cloud%20Computing\\_Outlook.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Outlook/Udo%20Helmbrecht_ENISA_Cloud%20Computing_Outlook.pdf)
- [4] <http://blogs.zdnet.com/security/?p=5110>
- [5] [http://voices.washingtonpost.com/securityfix/2008/07/amazon\\_](http://voices.washingtonpost.com/securityfix/2008/07/amazon_)
- [6] <http://www.programmableweb.com>
- [7] <http://securitylabs.websense.com/content/Blogs/3402.aspx>

- [8] Danielson, Krissi (2008-03-26). "Distinguishing Cloud Computing from Utility Computing". Ebizq.net. Retrieved 2010-08-22.
- [9] Gruman, Galen (2008-04-07). "What cloud computing really means". *InfoWorld*. Retrieved 2009-06-02.
- [10] "Cloud Computing: Clash of the clouds". *The Economist*. 2009-10-15. Retrieved 2009-11-03.
- [11] Cloud Computing Defined 17 July 2010. Retrieved 26 July 2010.
- [12] ."Writing & Speaking". Sellsbrothers.com. Retrieved 2010-08-22
- [13] "The Internet Cloud". *Thestandard.com*. Retrieved 2010-08-22.
- [14] Buyya, Rajkumar; Chee Shin Yeo, Srikumar Venugopal (PDF). *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities*. Department of Computer Science and Software Engineering, University of Melbourne, Australia. pp. 9. Retrieved 2008-07-31.
- [15] ""The Rise of Cloud Computing." Michael Otey. April 2010". windowsITpro.com. 2010-04-26. Retrieved 2010-08-22. "Google Apps is More Valuable than YouTube and Gmail Combined,