Cloud Computing Security Issues and Challenges

Tzouramanis Theodoros

Department of Electrical and Computer Engineering, University of the Aegean, Greece

Abstract: Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Advances in technologies and standards are allowing many types of more accurate patient data to be securely shared and analyzed across multiple devices and systems, and the impact on wellness monitoring and preventive care is revolutionary. The cloud landscape today consists of many independent and incompatible cloud vendors and providers. For each disparate cloud system, there are often multiple options, each with different externally visible interfaces, file formats, and operational conventions—and, in many cases, each of those utilize different semantics.

Keywords*:* Cloud computing, Virtualization, Grid computing, Hybrid cloud.

Introduction

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network. Cloud computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles.

The main enabling technology for cloud computing is virtualization. Virtualization software allows a physical computing device to be electronically separated into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors.

Users routinely face difficult business problems. Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.

Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loop in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery.

Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

Cloud computing shares characteristics with:

- Client–server model — *Client–server computing* refers broadly to any distributed application that distinguishes between service providers (servers) and service requestors (clients).

- Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."

- Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.

- Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."

- Peer-to-peer — A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo , Google etc. The consumer gets to use the software alone and enjoy the benefits.

Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. In June 2011, a study conducted by V1 found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept, highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average an 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs.

Cloud Computing Deployment Models and Concepts

Community Cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns, whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than that of a private) to realize its cost saving potential.

Public Cloud

A public cloud is established where several organizations have similar requirements and seek to share infrastructure so as to appliance. In addition, it can be economically attractive as the resources (storage, workstations) utilized and shared in the community are already exploited.

This is the cloud computing model where service providers make their computing resources available online for the public. It allows the users to access various important resources on cloud, such as: Software, Applications or Stored data. On of the prime benefits of using public cloud is that the users are emancipated from performing certain important tasks on their computing machines that they cannot get away with otherwise, these include: Installation of resources, their configuration; and Storage.

For obvious reasons, public cloud is bound to offer a multitude of benefits for its users, which can be sensed by its ubiquitous demand. Some of the most important ones are mentioned here:

1. Efficient storage and computing services

2. Inexpensive, since all the virtual resources whether application, hardware or data are covered by the service provider.

3. Allow for easy connectivity to servers and information sharing.

4. Assures appropriate use of resources as the users are required to pay only for the services they require.

5. Highly reliable and redundant.

6. Widespread availability irrespective of geographical precincts.

7. Sets the business people free from the hassles of buying, managing and maintaining all the virtual resources at their own end, the cloud server does it all.

8. Public cloud, in today's advanced workplace, empowers employees and enables them to become productive even when outside the office. The SaaS model ensures that corporations save on IT expenditures while delivering the flexibility of productivity software on the cloud.

Private cloud

iCylan APP enables you to remote access the sensitive applications of enterprises by smart phones or tablet device anywhere and anytime. The cloud-based resources are delivered to one platform, which providing high performance, security, and user experience. You can access the desktop, run applications, change settings, and access data exactly as you are sitting in front of the local PC, using its keyboard and mouse.

iCylan APP has three versions, such as Standard Edition, Advanced Edition, Enterprise Edition, which providing proven security of different class. It can connect to any Windows applications running a iCylan APP Client on smart phones or tablets devices. Nowadays, it supports the current systems, such as Google Android, Mac iOS, windows Phone 7 or BlackBerry.

Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

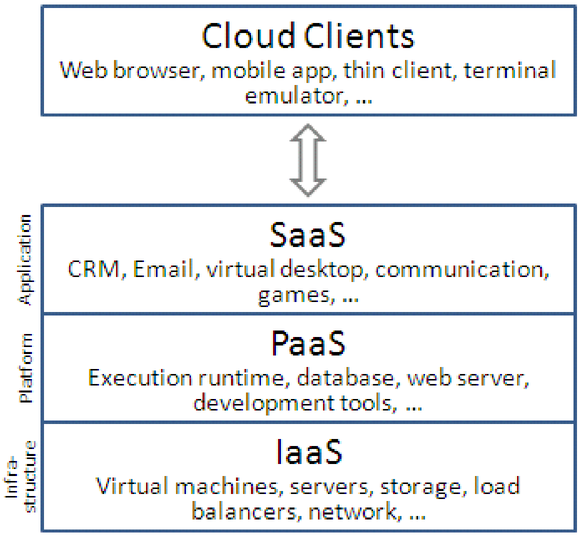
Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services.

Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that can not be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization only pays for extra compute resources when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

Service models

Cloud computing providers offer their services according to several fundamental models:


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, …
SaaS
CRM, Email, virtual desktop, communication, games, …
PaaS
Execution runtime, database, web server, development tools, …
IaaS
Virtual machines, servers, storage, load balancers, network, …
Application
Platform
Infra-structure

Infrastructure as a service (IaaS)

In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Xen, Oracle VirtualBox, KVM,VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.) IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks).

To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.

Platform as a service (PaaS)

In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.

Software as a service (SaaS)

In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee.

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications are different from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be *multitenant*, that is, any machine serves more than one cloud user organization.

The pricing model for SaaS applications is typically a monthly or yearly flat fee per user, so price is scalable and adjustable if users are added or removed at any point.

Proponents claim SaaS allows a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and personnel expenses, towards meeting other goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. One drawback of SaaS is that the users' data are stored on the cloud provider's server. As a result, there could be unauthorized access to the data. For this reason, users are increasingly adopting intelligent third-party key management systems to help secure their data.

Top threats to cloud computing security

Cloud computing has grabbed the spotlight at this year's RSA Conference 2013 in San Francisco, with vendors aplenty hawking products and services that equip IT with controls to bring order to cloud chaos. But the first step is for organization to identify precisely where the greatest cloud-related threats lie.

To that end, the CSA (Cloud Security Alliance) has identified "**The Notorious Nine**," the top nine cloud computing threats for 2013. The report reflects the current consensus among industry experts surveyed by CSA, focusing on threats specifically related to the shared, on-demand nature of cloud computing.

First on the list is data breaches. To illustrate the potential magnitude of this threat, CSA pointed to a research paper from last November describing how a virtual machine could **use side-channel timing information to extract private cryptographic keys** in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other clients' data as well.

The challenge in addressing this threats of data loss and data leakage is that "the measures you put in place to mitigate one can exacerbate the other," according to the report. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data. However, if you opt to keep offline backups of your data to reduce data loss, you increase your exposure to data breaches.

The second-greatest threat in a cloud computing environment, according to CSA, is data loss: the prospect of seeing your valuable data disappear into the ether without a trace. A malicious hacker might delete a target's data out of spite -- but then, you could lose your data to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting your data to ward off theft can backfire if you lose your encryption key.

Data loss isn't only problematic in terms of impacting relationships with customers, the report notes. You could also get into hot water with the feds if you're legally required to store particular data to remain in compliance with certain laws, such as HIPAA.

The third-greatest **cloud computing security risk** is account or service traffic hijacking. Cloud computing adds a new threat to this landscape, according to CSA. If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. "Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks," according to the report. As an example, CSA pointed to an XSS attack on Amazon in 2010 that let attackers hijack credentials to the site.

The key to defending against this threat is to protect credentials from being stolen. "Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible," according to CSA.

Fourth on the list of threats are insecure interfaces and APIs. IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency," the report notes.

CSA's advice here is for organizations to understand the security implications associated with the usage, management, orchestration, and **monitoring of cloud services**. Weak interfaces and APIs can expose an organization to such security issues pertaining to confidentiality, integrity, availability, and accountability.

Denial of service ranks as the fifth-greatest security threat to cloud computing. DoS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DoS outages can cost service providers customers *and* prove pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, he or she "may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself," the report says.

No. 6 on the list is malicious insiders, which can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From **IaaS** to **PaaS** to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryption is implement, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack," according to CSA.

Seventh on the list is cloud abuse, such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.

Eight on the list of top security threats to cloud computing is insufficient due diligence; that is, organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud. CSA's basic advice is for organizations to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud.

Last but not least, CSA has pegged shared technology vulnerabilities as the ninth-largest security threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models," according to the report.

If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to a potential of compromise and breach. CSA recommends a defensive, in-depth strategy, including compute, storage, network, application, and user security enforcement, as well as monitoring.

Cloud computing security

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data backup plan in the case of a cloud security breach.

Security issues associated with the cloud

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, and Hybrid). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must ensure that the provider has taken the proper security measures to protect their information, and the user must take measures to use strong passwords and authentication measures.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An 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 a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.

Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

Conclusion

Essentially securing an Information System (IS), involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability). Cloud computing due to its architectural design and characteristics imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. While many traditional risks are countered effectively, due to the infrastructures singular characteristics, a number of distinctive security challenges are introduced. Cloud computing has "unique attributes that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing"

References

"Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

Adams, Richard (2013). "'The emergence of cloud storage and the need for a new digital forensic process model". Murdoch University.

Bernstein, David; Ludvigson, Erik; Sankar, Krishna; Diamond, Steve; Morrow, Monique (2009-05-24). "Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability". *Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability*. IEEE Computer Society. pp. 328–336.

Dario Bruneo, Salvatore Distefano, Francesco Longo, Antonio Puliafito, Marco Scarpa: Workload-Based Software Rejuvenation in Cloud Systems. IEEE Trans. Computers 62(6): 1072-1085 (2013)

HAMDAQA, Mohammad (2012). *Cloud Computing Uncovered: A Research Landscape*. Elsevier Press. pp. 41–85.

He, Sijin; L. Guo; Y. Guo; C. Wu; M. Ghanem; R. Han.*Elastic Application Container: A Lightweight Approach for Cloud Resource Provisioning*. 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA). pp. 15–22.

Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80.

oorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In R. Buyya, J. Broberg, A.Goscinski. *Cloud Computing: Principles and Paradigms*. New York, USA: Wiley Press. pp. 1–44.

Strachey, Christopher (June 1959). "Time Sharing in Large Fast Computers". *Proceedings of the International Conference on Information processing, UNESCO*. paper B.2.19: 336–341.

Vincenzo D. Cunsolo, Salvatore Distefano, Antonio Puliafito, Marco Scarpa: Volunteer Computing and Desktop Cloud: The Cloud@Home Paradigm. IEEE International Symposium on Network Computing and Applications, NCA 2009, pp 134-139

Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. p. 59.

Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. pp. 65, 68, 72, 81, 218–219, 231, 240.