International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

Privacy and Security issues in Cloud Computing

Anita Kumari Nanda[1], Brojo Kishore Mishra[2]
[1]Department of Basic Science, [2]Department of Computer Science
[1,2]MITS Institute of Polytechnic (MIP), Rayagada, India

Abstract

"Cloud computing" – a relatively recent term, defines the paths ahead in computer science world. Being built on decades of research it utilizes all recent achievements in virtualization, distributed computing, utility computing, and networking. It implies a service oriented architecture through offering software and platforms as services, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on demand services and many other things. Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation. This paper is a brief survey based on readings of "cloud" computing and it tries to address related research topics, privacy and security issues ahead and possible solution.

Keywords

Cloud Computing, Data Security, PAAS, SAAS.

1. Introduction

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Several computing paradigms have promised to deliver this utility computing vision and these include cluster computing, Grid computing, and more recently Cloud computing. The latter term denotes the infrastructure as a "Cloud" from which businesses and users are able to access applications from anywhere in the world on demand. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than to run on their individual computers.

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The Internet is often represented as a cloud and the term "cloud computing" arises from that analogy. Accenture defines cloud computing as the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network. Cloud computing is the need of today's business 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 storage, memory, processing and bandwidth. Traditional business applications of various companies have always been too complicated and expensive because they run a data centre with office space, power, cooling, bandwidth, networks, servers, and storage. A complicated software stack and a team of experts to install, configure, and run them. They need development, testing, staging, production, and failover environments. These headaches across dozens or hundreds of applications grow in a multiplicative way. It gives a solid reason to the biggest companies with the best IT departments to run their application on a central data centre by using different clouds. When an application runs in the cloud, customer just logs in, customize the application, and start using it on a pool data centre with the power of cloud computing. Today's Businesses are running all kinds of applications in the cloud these days. They cost less, because there is no need to pay for all the people, products, and facilities to run them. Clouds turns out more scalable, more secure, and more reliable than most applications. Additionally, upgrades are taken care so that applications get security and performance enhancements and new features automatically. The way a consumer pay for cloud-based apps is also different. Forget about buying servers and software. When consumer's applications run in the cloud, consumer buys nothing. It is available with a predictable monthly subscription, so consumers only pay for what is actually used.

2. Cloud Computing

The term "cloud", as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. "Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form 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.

The literature identifies four different broad service models for cloud computing:

- Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality
- Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software)
- Infrastructure as a Service (IaaS), where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services.
- Hardware as a Service (HaaS), where the cloud provides access to dedicated firmware via the Internet

Cloud computing offerings also differ by scope. In private clouds, services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organization's data centre delivers cloud computing services to clients who may or may not be in the premises. Public clouds are the opposite: services are offered to individuals and organizations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures. Public cloud users are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings.

3. Characteristics of Cloud Computing

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data-enter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

4. Advantages and Disadvantages of Cloud Computing

A. Advantages :

- Lower computer costs:
  - You do not need a high-powered and high-priced computer to run cloud computing web-based applications.
  - Since applications run in the cloud, not on the desktop PC, your desktop PC does not need the processing power or hard disk space demanded by traditional desktop software.

  - When you are using web-based applications, your PC can be less expensive, with a smaller hard disk, less memory, more efficient processor...
  - In fact, your PC in this scenario does not even need a CD or DVD drive, as no software programs have to be loaded and no document files need to be saved.
- Improved performance:
  - With few large programs hogging your computer's memory, you will see better performance from your PC.
  - Computers in a cloud computing system boot and run faster because they have fewer programs and processes loaded into memory.
- Reduced software costs:
  - Instead of purchasing expensive software applications, we can get most of what you need for free.
  - That is right - most cloud computing applications today, such as the Google Docs suite, are totally free.
- Instant software updates:
  - Another advantage to cloud computing is that you are no longer faced with choosing between obsolete software and high upgrade costs.
  - When the application is web-based, updates happen automatically - available the next time you log into the cloud.
  - When you access a web-based application, you get the latest version - without needing to pay for or download an upgrade.
- Improved document format compatibility.
  - You do not have to worry about the documents you create on your machine being compatible with other users' applications or operating systems.
  - Where Word 2007 documents cannot be opened on a computer running Word 2003, all documents can be read!
- Unlimited storage capacity:
  - Cloud computing offers virtually limitless storage.
  - Whatever you need to store, you can.
- Increased data reliability:
  - Unlike desktop computing, in which if a hard disk crashes and destroy all your valuable data, a computer crashing in the cloud should not affect the storage of your data.
  - That also means that if your personal computer crashes, all your data is still out there in the cloud, still accessible.
  - In a world where few individual desktop PC users back up their data on a regular basis, cloud computing is a data-safe computing platform!
- Universal document access:
  - That is not a problem with cloud computing, because you do not take your documents with you.
  - Instead, they stay in the cloud, and you can access them whenever you have a computer and an Internet connection.
  - All your documents are instantly available from wherever you are.
- Latest version availability:
  - Another document-related advantage of cloud computing is that when you edit a document at home, that edited version is what you see when you access the document at work.
  - The cloud always hosts the latest version of your documents; as long as you are connected, you are not in danger of having an outdated version.
- Easier group collaboration:
  - Sharing documents leads directly to better collaboration.
  - Many users do this as it is an important advantages of cloud computing - multiple users can collaborate easily on documents and projects.
  - Because the documents are hosted in the cloud, not on individual computers, all you need is an

Internet connection, and you are collaborating.
- Device independence.
  - You are no longer tethered to a single computer or network.
  - Changes to computers, applications and documents follow you through the cloud.
  - Move to a portable device, and your applications and documents are still available.

B. Disadvantages:
- Requires a constant Internet connection:
  - Cloud computing is impossible if you cannot connect to the Internet.
  - Since you use the Internet to connect to both your applications and documents, if you do not have an Internet connection you cannot access anything, even your own documents.
  - A dead Internet connection means no work and in areas where Internet connections are few or inherently unreliable, this could be a deal-breaker.
  - When you are offline, cloud computing simply does not work.
- Does not work well with low-speed connections:
  - Similarly, a low-speed Internet connection, such as that found with dial-up services, makes cloud computing painful at best and often impossible.
  - Web-based applications require a lot of bandwidth to download, as do large documents.
  - If you are laboring with a low-speed dial-up connection, it might take seemingly forever just to change from page to page in a document, let alone to launch a feature-rich cloud service.
- Can be slow:
  - Even with a fast connection, web-based applications can sometimes be slower than accessing a similar software program on your desktop PC.
  - Everything about the program, from the interface to the current document, has to be sent back and forth from your computer to the computers in the cloud.
  - If the cloud servers happen to be backed up at that moment, or if the Internet is having a slow day, you would not get the instantaneous access you might expect from desktop applications.
- Features might be limited:
  - This situation is bound to change, but today many web-based applications simply are not as full-featured as their desktop-based applications.
  - For example, you can do a lot more with Microsoft PowerPoint than with Google Presentation's web-based offering.
  - The basics are similar, but the cloud application lacks many of PowerPoint's advanced features.
  - If you are a power user, you might not want to leap into cloud computing just yet.
- Stored data might not be secure:
  - Cloud computing companies say that data is secure, but it is too early to be completely sure of that.
  - Only time will tell if your data is secure in the cloud.
- Stored data can be lost:
  - Theoretically, data stored in the cloud is safe, replicated across multiple machines.
  - But on the off chance that your data goes missing, you have no physical or local backup.
  - Put simply, relying on the cloud puts you at risk if the cloud lets you down.
- HPC Systems:
  - Not clear that you can run compute-intensive HPC applications that use MPI/OpenMP.
  - Scheduling is important with this type of application – as you want all the VM to be co-located to minimize communication latency!
- General Concerns:
  - Each cloud systems use different protocols and different APIs… so it may not be possible to run

applications between cloud based systems.
- Amazon has created its own DB system (not SQL 92), and workflow system (many popular workflow systems out there) – so your normal applications will have to be adapted to execute on these platforms.

5. Privacy and Security issues in Cloud Computing

Shared infrastructure scares many enterprise customers. Depending on the type of cloud computing used (IaaS or PaaS) and the level of abstraction (OS-level vs. platform vs. Application level) different security issues arise in public clouds. The cloud provider is responsible for the physical security of the machines, for ensuring that VM instances are running isolated from one another (i.e. crashes and software exploits of one system do not affect the others) as well as for setting up firewalls to protect the VM machines from the network. However, higher level cloud services such as Google AppEngine and platforms like Azure are also responsible for their application-level security and clients have less control controlling it. In addition, downtimes, outright data losses in storage services and risks of cloud provider malfeasance are further threats to be weighted when a company considers public cloud services usage.

Data Security – Confidentiality and Availability: VMs have shown vulnerabilities to certain kinds of memory attacks (UC Berkeley points to research at Princeton that shows how Java and .NET VMs could be hijacked by inducing memory errors. Even though physical access to the PC running the VM is a prerequisite, I argue that private clouds are generally more secure, as availability of the physical machines and full administrative rights are at the company's disposal. Arguably, it is much more likely that in case a bug is found (or proactively with malicious attacks) problems arise that allow VM users to access other users' VM instances or storage data. Naturally, such problems exist in large data-centers too, yet the implications of ultra large scale failures given hundreds of thousands of potential cloud users sharing the same infrastructure could be devastating. Debugging such distributed such developed; widely distributed systems may later be very difficult, as some errors could not be reproduced in smaller, test configurations. Encrypted all data sent to the cloud may be an option to ensure security, yet this may have implications on costs for developing/configuring applications appropriately.

Cloud Provider Malfeasance: Cloud provider malfeasance refers to the operational counterparty risk associated with misuse, data theft or malicious altering of confidential customer data by the cloud service vendor. The cloud provider is the ultimate administrative entity and is able to effortlessly spy (including to log, analyze etc.) on VMs and storage data of the underlying instances in the cloud. This is particularly relevant for large enterprises, although one can argue that such large companies would move to the cloud only parts of their compute/storage tasks and will have separate confidentiality agreements with the cloud provider. Yet the sheer amount of business (and even technologically) sensitive data that cloud providers are able to trace and potentially take advantage of must be considered, given that large public cloud providers envision massive future usage and entire IT-departments allocated in the cloud. Moreover, involuntary or accidental data exposure could also occur (e.g. Amazon's S3 outage in 2006 when users could see other user's data.

Uptime Guarantees: Six Amazon (EC2 compute and S3 storage) downtimes lasting 1.5 – 8 hours as well as Google AppEngine and Gmail outages are often quoted. Although uptimes from 99,9 – 99,95% are less than what most companies require, it is not clear whether most companies really need to set their SLA higher than 99,99% (assumed monthly percentage availability required by a large enterprise from a typical/own data-center).
As with every distributed system, Cloud Computing has lots of problems. We have to take care of the network infrastructure, which is not always in our control, and very careful with the data in order to avoid third parties from capturing it. Some security solutions and problems have been proposed by ArmMichael Halton:

- Web application vulnerabilities: Cross scripting, SQL injections. Solution: Develop a security oriented framework that teaches the best programming practices.
- Vulnerabilities inherent to the TCP/IP stack and/or the operating systems: DoS, and DDos(Distributed denial of service). Solution: Deactivate unused services, update applications and control rights.

- Authentication problems: IP spoofing, RIP attacks, ARP poisoning. Solution: Use encrypted protocols if possible prevents IP spoofing, controlling rights to access ARP tables, etc.
- The verification, tampering and loss of data. Solution: encrypted data would be a solution, but, 'since the unencrypted data must reside in the memory of the host running the computation'; this must be encrypted in order to avoid memory copies.
- Physical access. Solution: Control rights and log actions when accessing the hardware.
- Privacy control of data. Solution: Use Service-level agreements.

6. Conclusion

Cloud computing is undoubtedly still work in progress – both from a technical and business perspective. In emphasizing the cost and performance benefits of the cloud, some fundamental security problems have receded into the background and been left unresolved. Several critical pieces of technology, such as a solution for federated trust, are not yet fully realized, impinging on successful deployments. Determining the security of complex computer systems is also a long-standing security problem that overshadows large scale computing in general. Attaining the high assurance qualities in implementations has been an elusive goal of computer security researchers and practitioners, and is also a work in progress for cloud computing.
Security of the cloud infrastructure relies on trusted computing and cryptography. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. No standard service contract exists that covers the ranges of cloud services available and the needs of different organizations. Having a list of common outsourcing provisions, such as privacy and security standards, regulatory and compliance issues, service level requirements and penalties, change management processes, continuity of service provisions, and termination rights, provides a useful starting point.

Acknowledgment

The author would like to thank the MITS Institute of Polytechnic and Prof. Asutosh, ACCENTS for encouraging this paper to publish.

References

[1] Computing in the Clouds. Networker, 11(4):16-25, Dec. 2007.
[2] Boss G., Malladi P., Quan D., Legregni L., Hall H.; IBM on Cloud Computing; High Performance On-Demand Solutions, IBM; 8th Oct 2007.
[3] Buyya R., Yeo C.S., Venugopal S.; Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, Keynote Paper, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Sept. 25-27, 2008, Dalian, China.
[4] Chappell D.; Cloud Platforms Today: A Perspective; http://www.davidchappell.com/CloudPlatformsToday--APerspective-Chappell.pdf; 18 Apr 2009.
[5] Hamilton. 'Cloud computing' seen as next wave for technology investors. Financial Post, 4 June 2008.
[6] Erenben C.; Cloud Computing: The Economic Imperative; IBM e-School News; www.ibm.com/education, Mar 2009.
[7] Govindavajhala S., Appel A.; Using Memory Errors to Attack a Virtual Machine; 2003 IEEE Symposium on Security and Privacy, pp. 154-165, May 2003.
[8] J. Broberg, R. Buyya, and Z. Tari. MetaCDN: Harnessing 'Storage Clouds' for High Performance Content Delivery. Technical Report GRIDS-TR-2008-11, Grid Computing and Distributed Systems Laboratory, the University of Melbourne, Australia, 15 Aug. 2008.

Miss Anita Nanda, Faculty, Department of Basic Science, MITS Institute of Polytechnic, Rayagada-765017, Odisha, India. Her area of interest is Soft Computing, Cloud Computing.

Dr. Brojo Kishore Mishra, Faculty, Department of Computer Science & Engg, MITS Institute of Polytechnic, Rayagada-765017, Odisha, India. His area of interest is Cloud Computing, Data / Web Mining, Soft Computing.