RESEARCH ARTICLE OPEN ACCESS

Hosting Services by Cloud Computing

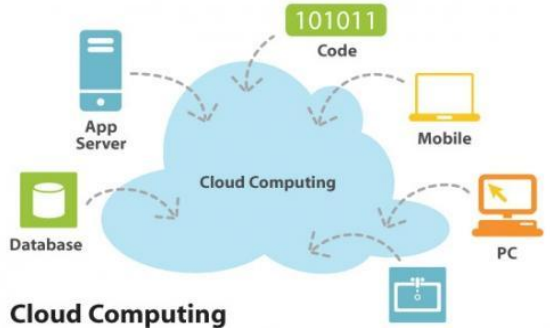
A. Mallikarjuna[1], S. Madhuri[2]
[1]*Research Scholar, Dept. of Computer Science, S.V. University, Tirupati, Andhra Pradesh.*
[2]*Dept. of Information Technology,JNTU, Hyderabad, Andhra Pradesh.*

Abstract
Cloud computing is basically an Internet-based network made up of large numbers of servers - mostly based on open standards, modular and inexpensive. Clouds contain vast amounts of information and provide a variety of services to large numbers of people. The benefits of cloud computing are Reduced Data Leakage, Decrease evidence acquisition time, they eliminate or reduce service downtime, they Forensic readiness, they Decrease evidence transfer time. The main factor to be discussed is security of cloud computing, which is a risk factor involved in major computing fields.
Keywords: Metaphor, data leakage, forensic, cloud, hosted services.

I. Introduction

What is a Cloud computing?

Cloud computing is Internet- ("CLOUD-") based development and use of computer technology("COMPUTING").
Cloud computing is a general term for anything that involves delivering hosted services over the Internet.
It is used to describe both a platform and type of application.
Cloud computing also describes applications that are extended to be accessible through the Internet.
These cloud applications use large data centers and powerful servers that host Web applications and Web services.
Anyone with a suitable Internet connection and a standard browser can access a cloud application.



User of the cloud only care about the service or information they are accessing - be it from their PCs, mobile devices, or anything else connected to the Internet - not about the underlying details of how the cloud works.

History:

The Cloud is a metaphor for the Internet, derived from its common depiction in network diagrams (or more generally components which are managed by others) as a cloud outline. The underlying concept dates back to 1960 when John McCarthy opined that "computation may someday be organized as a public utility" (indeed it shares characteristics with service bureaus which date back to the 1960s) and the term The Cloud was already in commercial use around the turn of the 21st century. Cloud computing solutions had started to appear on the market, though most of the focus at this time was on Software as a service. 2007 saw increased activity, including Goggle, IBM And a number of universities embarking on a large scale cloud computing research project, around the time the term started gaining popularity in the main stream press. It was a hot topic by mid-2008 and numerous cloud computing events had been scheduled.

II. WHAT IS DRIVING CLOUD COMPUTING?

The CLOUD COMPUTING is driving in two types of categories .They are as follows:
1. Customer perspective
2. Vendor perspective

1. Customer perspective:

In one word: economics Faster, simpler, cheaper to use cloud computation. No upfront capital required for servers and storage. No ongoing for operational expenses for running data center. Application can be run from anywhere.

2. Vendor perspective:

Easier for application vendors to reach new Customers. Lowest cost way of delivering and supporting applications. Ability to use commodity server and storage hardware. Ability to drive down data center operational cots.

Types of services:
These services are broadly divided into three categories:

- *Infrastructure-as-a-Service* ***(IaaS)***
- *Platform-as-a-Service* ***(PaaS)***
- *Software-as-a-Service* ***(SaaS).***

Infrastructure-as-a-Service (IaaS):

Infrastructure-as-a-Service(IaaS) like Amazon Web Services provides virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an API from which they can control their servers. Because customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.

Platform-as-a-Service (PaaS):

Platform-as-a-Service(PaaS) is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. Google Apps is one of the most famous Platform-as-a-Service providers. Developers should take notice that there aren't any interoperability standards (yet), so some providers may not allow you to take your application and put it on another platform.

Software-as-a-Service (SaaS):

Software-as-a-Service (SaaS) is the broadest market. In this case the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from web based email, to applications like Twitter or Last.fm.

Types by visibility:

Public cloud:

Public *cloud* or *external cloud* describes cloud

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

Hybrid cloud:

A *hybrid cloud* environment consisting of multiple internal and/or external providers[1] "will be typical for most enterprises. A hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, colocated assets—for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

Private cloud:

Private cloud and *internal cloud* are neologisms that some vendors have recently used to describe offerings that emulate cloud computing on private networks. These (typically virtualisation automation) products claim to "deliver some benefits of cloud computing without the pitfalls", capitalising on data security, corporate governance, and reliability concerns. They have been criticized on the basis that users "still have to buy, build, and manage them". and as such do not benefit from lower up-front capital costs and less hands-on management[f], essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

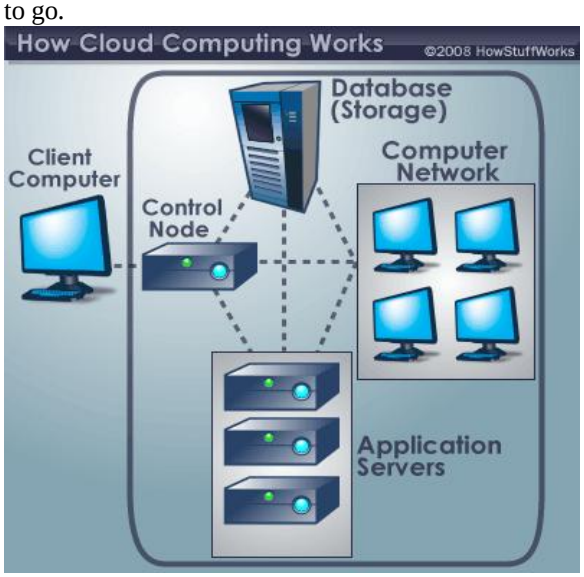
While an analyst predicted in 2008 that private Cloud networks would be the future of corporate IT, there is some uncertainty whether they are a reality even within the same firm. Analysts also claim that within five years a "huge percentage" of small and medium enterprises will get most of their computing resources from external cloud computing providers as they "will not have economies of scale to make it worth staying in the IT business" or be able to afford private clouds. Analysts have reported on Platform's view that private clouds are a stepping stone to external clouds, particularly for the financial services, and that future datacenters will look like internal clouds. The term has also been used in the logical rather than physical sense, for example in reference to platform as a service offerings, though such offerings including Microsoft's Azure Services Platform are not available for on-premises deployment.

How does cloud computing work?

Supercomputers today are used mainly by the military, government intelligence agencies, universities and research labs, and large companies to tackle enormously complex calculations for such tasks as simulating nuclear explosions, predicting climate change, designing airplanes, and analyzing which proteins in the body are likely to bind with potential new drugs. Cloud computing aims to apply that kind of power—measured in the tens of trillions of computations per second—to problems like analyzing risk in financial portfolios, delivering personalized medical information, even powering immersive computer games, in a way that users can tap through the Web. It does that by networking large groups of Servers that often use low-cost consumer PC technology, with specialized connections to spread data-processing chores across them.

By contrast, the newest and most powerful desktop PCs process only about 3 billion computations a second. Let's say you're an executive at a large corporation. Your particular responsibilities include making sure that all of your employees have the right

hardware and software they need to do their jobs. Buying computers for everyone isn't enough -- you also have to purchase software or software licenses to give employees the tools they require. Whenever you have a new hire, you have to buy more software or make sure your current software license allows another user. It's so stressful that you find it difficult to go.

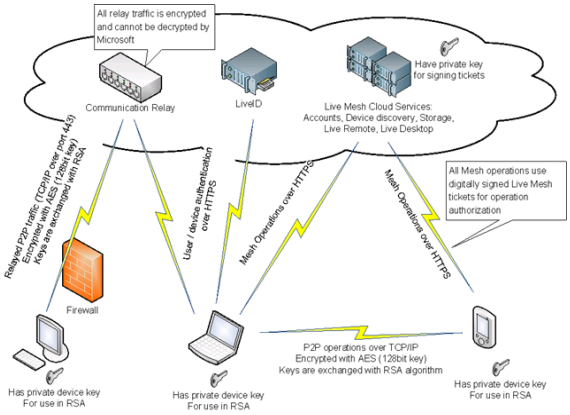


A typical cloud computing system

Soon, there may be an alternative for executives like you. Instead of installing a suite of software for each computer, you'd only have to load one application. That application would allow workers to log into a Web-based service which hosts all the programs the user would need for his or her job. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs.

It's called cloud computing**,** and it could change the entire computer industry. In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloudcomputing system's interface software**,** which can be as simple as a Web browser, and the cloud's network takes care of the rest. There's a good chance you've already used some form of cloud computing. If you have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then you've had some experience with cloud computing. Instead of running an e-mail program on your computer, you log in to a Web e-mail account remotely. The software and storage for your account doesn't exist on your computer -- it's on the service's computer cloud.

III. SEVEN TECHNICAL SECURITY BENEFITS OF THE CLOUD:



1. CENTRALIZED DATA:

Reduced Data Leakage: this is the benefit I hear most from Cloud providers - and in my view they are right. How many laptops do we need to lose before we get this? How many backup tapes? The data "landmines" of today could be greatly reduced by the Cloud as thin client technology becomes prevalent. Small, temporary caches on handheld devices or Netbook computers pose less risk than transporting data buckets in the form of laptops. Ask the CISO of any large company if all laptops have company 'mandated' controls consistently applied; e.g. full disk encryption. You'll see the answer by looking at the whites of their eyes. Despite best efforts around asset management and endpoint security we continue to see embarrassing and disturbing misses. And what about SMBs? How many use encryption for sensitive data, or even have a data classification policy in place?

Monitoring benefits: central storage is easier to control and monitor. The flipside is the nightmare scenario of comprehensive data theft. However, I would rather spend my time as a security professional figuring out smart ways to protect and monitor access to data stored in one place (with the benefit of situational advantage) than trying to figure out all the places where the company data resides across a myriad of thick clients! You can get the benefits of Thin Clients today but Cloud Storage provides a way to centralize the data faster and potentially cheaper. The logistical challenge today is getting Terabytes of data to the Cloud in the first place.

2. INCIDENT RESPONSE / FORENSICS:

Forensic readiness: with Infrastructure as a Service (IaaS) providers, I can build a dedicated forensic server in the same Cloud as my company and place it offline, ready for use when needed. I would only need pay for storage until an incident happens and I need to bring it online. I don't need to call someone to bring it online or install some kind of remote boot software - I just click a button in the Cloud Providers web interface. If I have multiple incident responders,

I can give them a copy of the VM so we can distribute the forensic workload based on the job at hand or as new sources of evidence arise and need analysis. To fully realise this benefit, commercial forensic software vendors would need to move away from archaic, physical dongle based licensing schemes to a network licensing model.

Decrease evidence acquisition time: if a server in the Cloud gets compromised (i.e. broken into), I can now clone that server at the click of a mouse and make the cloned disks instantly available to my Cloud Forensics server. I didn't need to "find" storage or have it "ready, waiting and unused"- its just there.

Eliminate or reduce service downtime: Note that in the above scenario I didn't have to go tell the COO that the system needs to be taken offline for hours whilst I dig around in the RAID Array hoping that my physical acqusition toolkit is compatible (and that the version of RAID firmware isn't supported by my forensic software). Abstracting the hardware removes a barrier to even doing forensics in some situations.

Decrease evidence transfer time: In the same Cloud, bit fot bit copies are super fast - made faster by that replicated, distributed file system my Cloud provider engineered for me. From a network traffic perspective, it may even be free to make the copy in the same Cloud. Without the Cloud, I would have to a lot of time consuming and expensive provisioning of physical devices. I only pay for the storage as long as I need the evidence.

Eliminate forensic image verification time:
Some Cloud Storage implementations expose a cryptographic checksum or hash. For example, Amazon S3 generates an MD5 hash automagically when you store an object. In theory you no longer need to generate time-consuming MD5 checksums using external tools - it's already there.

Decrease time to access protected documents:
Immense CPU power opens some doors. Did the suspect password protect a document that is relevant to the investigation? You can now test a wider range of candidate passwords in less time to speed investigations.

3. PASSWORD ASSURANCE TESTING (AKA CRACKING):

Decrease password cracking time: if your organization regularly tests password strength by running password crackers you can use Cloud Compute to decrease crack time and you only pay for what you use. Ironically, your cracking costs go up as people choose better passwords;-).

Keep cracking activities to dedicated machines: if today you use a distributed password cracker to spread the load across non-production machines, you can now put those agents in dedicated Compute instances - and thus stop mixing sensitive credentials with other workloads.

4. LOGGING:

"Unlimited", pay per drink storage: logging is often an afterthought, consequently insufficient disk space is allocated and logging is either non- existant or minimal. Cloud Storage changes all this - no more 'guessing' how much storage you need for standard logs.

Improve log indexing and search: with your logs in the Cloud you can leverage Cloud Compute to index those logs in real-time and get the benefit of instant search results. What is different here?
The Compute instances can be plumbed in and scale as needed based on the logging load – meaning a true real-time view.

Getting compliant with Extended logging: most modern operating systems offer extended logging in the form of a C2 audit trail. This is rarely enabled for fear of performance degradation and log size. Now you can 'opt-in' easily - if you are willing to Pay for the enhanced logging, you can do so. Granular logging makes compliance and investigations easier.

5. IMPROVE THE STATE OF SECURITY SOFTWARE (PERFORMANCE):

Drive vendors to create more efficient security software: Billable CPU cycles get noticed. More attention will be paid to inefficient processes; e.g. poorly tuned security agents. Process accounting will make a comeback as customers target 'expensive' processes. Security vendors that understand how to squeeze the most performance from their software will win.

6. SECURE BUILDS:

Pre-hardened, change control builds: this is primarily a benefit of virtualization based Cloud Computing. Now you get a chance to start 'secure' (by your own definition) - you create your Gold Image VM and clone away. There are ways to do this today with bare-metal OS installs but frequently these require additional 3rd party tools, are time consuming to clone or add yet another agent to each endpoint.

Reduce exposure through patching offline: Gold images can be kept up securely kept up to date. Offline VMs can be conveniently patched "off" the network.

Easier to test impact of security changes: this is a big one. Spin up a copy of your production

environment, implement a security change and test the impact at low cost, with minimal startup time. This is a big deal and removes a major barrier to 'doing' security in production environments.

7. SECURITY TESTING:

Reduce cost of testing security: a SaaS provider only passes on a portion of their security testing costs. By sharing the same application as a service, you don't foot the expensive security code review and/or penetration test. Even with Platform as a Service (PaaS) where your developers get to write code, there are potential cost economies of scale (particularly around use of code scanning tools that sweep source code for security weaknesses).

Adoption fears and strategic innovation opportunities

Adoption-fears **Security**: Many IT executives make decisions based on the perceived security risk instead of the real security risk. IT has traditionally feared the loss of control for SaaS deployments based on an assumption that if you cannot control something it must be unsecured. I recall the anxiety about the web services deployment where people got really worked up on the security of web services because the users could invoke an internal business process from outside of a firewall. The IT will have to get used to the idea of software being delivered outside from a firewall that gets meshed up with on-premise software before it reaches the end user. The intranet, extranet, DMZ, and the internet boundaries have started to blur and this indeed imposes some serious security challenges such as relying on a cloud vendor for the physical and logical security of the data, authenticating users across firewalls by relying on vendor's authentication schemes etc., but assuming challenges as fears is not a smart strategy.

Latency: Just because something runs on a cloud it does not mean it has latency. My opinion is quite the opposite. The cloud computing if done properly has opportunities to reduce latency based on its architectural advantages such as massively parallel processing capabilities and distributed computing. The web-based applications in early days went through the same perception issues and now people don't worry about latency while shopping at Amazon.com or editing a document on Google docs served to them over a cloud. The cloud is going to get better and better and the IT has no strategic advantages to own and maintain the data centers. In fact the data centers are easy to shut down but the applications are not and the CIOs should take any and all opportunities that they get to move the data centers away if they can.

SLA: Recent Amazon EC2 meltdown and RIM's network outage created a debate around the availability of a highly centralized infrastructure and their SLAs. The real problem is not a bad SLA but lack of one. The IT needs a phone number that they can call in an unexpected event and have an up front estimate about the downtime to manage the expectations. May be I am simplifying it too much but this is the crux of the situation. The fear is not so much about 24x7availability since an on-premise system hardly promises that but what bothers IT the most is inability to quantify the impact on business in an event of non-availability of a system and set and manage expectations upstream and downstream. The non-existent SLA is a real issue and I believe there is a great service innovation opportunity for ISVs and partners to help CIOs with the adoption of the cloud computing by providing a rock solid SLA and transparency into the defect resolution process.

Strategic innovation opportunities

Seamless infrastructure virtualization:

If you have ever attempted to connect to Second Life behind the firewall you would know that it requires punching few holes into the firewall to let certain unique transports pass through and that's not a viable option in many cases. This is an intra-infrastructure communication challenge. I am glad to see IBM's attempt to create a virtual cloud inside firewall to deploy some of the regions of the Second Life with seamless navigation in and out of the firewall. This is a great example of a single sign on that extends beyond the network and hardware virtualization to form infrastructure virtualization with seamless security.

Hybrid systems: The IBM example also illustrates the potential of a hybrid system that combines an on-premise system with remote infrastructure to support seamless cloud computing.

This could be a great start for many organizations that are on the bottom of the S curve of cloud computing adoption. Organizations should consider pushing non-critical applications on a cloud with loose integration with on-premise systems to begin the cloud computing journey and as the cloud infrastructure matures and some concerns are alleviated IT could consider pushing more and more applications on the cloud. Google App Engine for cloud computing is a good example to start creating applications on-premise that can eventually run on Google's cloud and Amazon's AMI is expanding day-by-day to allow people to push their applications on Amazon's cloud. Here is a quick comparison of Google and Amazon in their cloud computing efforts. Elastra's solution to deploy Enterprise DB on the cloud is also a good example of how organizations can outsource IT on the cloud.

IV. BENEFITS

Cloud computing infrastructures can allow enterprises to achieve more efficient use of their IT Hardware and software investments. They Do this by

breaking down the physical inherent in isolated systems, and automating the management of the group of systems as a single entity. Cloud computing is an example of an ultimately virtualized system, and a natural evolution for Data centers that employ automated systems management, workload balancing, and virtualization technologies. A cloud infrastructure can be a cost efficient model for delivering information services

V. Application

A ***cloud application*** leverages cloud computing in software architecture, often eliminating the need to install and run the application on the customer's own computer, thus alleviating the burden of software maintenance, ongoing operation, and support. For example:

- Peer-to-peer / volunteer computing (BOINC, Skype)
- Web applications (Webmail, Facebook, Twitter, YouTube, Yammer)
- Security as a service (MessageLabs, Purewire, ScanSafe, Zscaler)
- Software as a service (Google Apps, Salesforce,Nivio,Learn.com, Zoho, BigGyan. com)
- Software plus services (Microsoft Online Services)
- Storage [Distributed]
  - Content distribution (BitTorrent, Amazon CloudFront)
  - Synchronisation (Dropbox, Live Mesh, SpiderOak, ZumoDrive)

VI. CONCLUSION

In my view, there are some strong technical security arguments in favour of Cloud Computing - assuming we can find ways to manage the risks. With this new paradigm come challenges and opportunities. The challenges are getting plenty of attention - I'm regularly afforded the opportunity to comment on them, plus obviously I cover them on this blog. However, let's not lose sight of the potential upside.

Some benefits depend on the Cloud service used and therefore do not apply across the board. For example; I see no solid forensic benefits with SaaS. Also, for space reasons, I'm purposely not including the 'flip side' to these benefits, however if you read this blog regularly you should recognise some.

We believe the Cloud offers Small and Medium Businesses major potential security benefits. Frequently SMBs struggle with limited or non-existent. in-house INFOSEC resources and budgets. The caveat is that the Cloud market is still very new – security offerings are somewhat foggy – making selection tricky. Clearly, not all Cloud providers will offer the same security.

REFERENCES

[1]. **Web guild.org** http://www.webguild.org/
[2]. **How stuff works.com** http://communication.howstuffworks.com/
[3]. **Cloud security.org** http://cloudsecurity.org
[4]. **IBM** http://www.ibm.com/developerworks /websphere/zones/hipods/
[5]. **Google suggest** http://www.google.com/webhp?complete=1& hl=en