

ClubHACKMag



ITS THERE, UP IN THE CLOUDS

WHERE THE HECK IS MY DATA



Issue 8 | Sep 2010
www.chmag.in

1st Indian "HACKING" Magazine

TechGyan Cloud Computing Security Threats | **LegalGyan** CLOUD & LAW | **ToolGyan** CLOUDSHARK | **Mom's Guide** WHAT THE HECK IS CLOUD |

Its rainy season here in India, and the clouds are all over the sky and now in this issue too, yes the cover page I designed says it all, this issue is specially on Cloud Computing, now see your data safe in the clouds until it rains.. Just kidding :P

This issue will cover topics on Cloud computing security & threats in Tech Gyan, Cloud & law in Legal Gyan, Cloud shark in Tool Gyan and in Mom's Guide for the people who have a question what the heck is cloud?

And the dates for the big event ClubHack Conference 2010 are 4th, 5th & 6th December 2010, Hope the interested one's

have submitted their CFP for it, If not then visit <http://clubhack.com/2010/cfp/>



Pankit Thakkar

ClubHACKMag

Issue 8, Sep 2010.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Deepranjan S More
deepranjan@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Pg **TechGyan**
03 Cloud Computing Security & Threats

Pg **ToolGyan**
13 CLOUDSHARK

Pg **Mom'sGuide**
16 WHAT THE HECK IS CLOUD

Pg **LegalGyan**
19 CLOUD & LAW

Pg **Command LineGyan**
21 USING CLOUD FROM
COMMAND SHELL



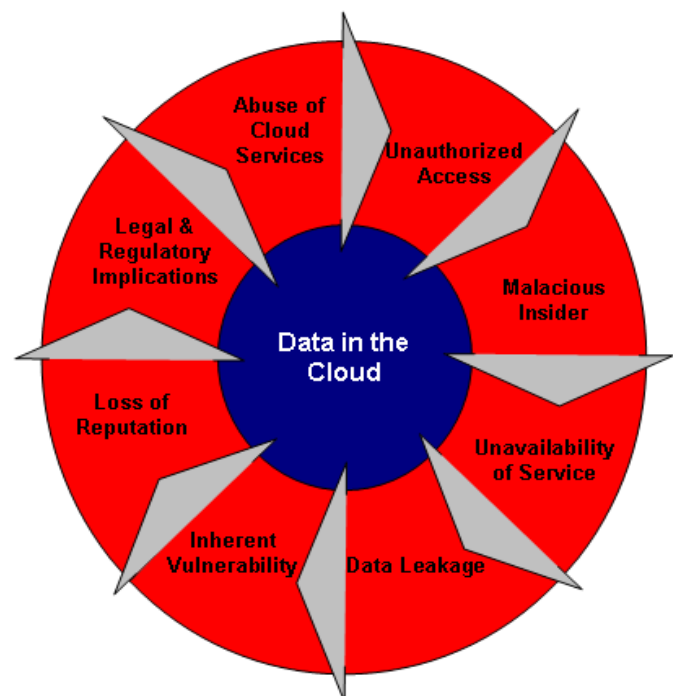
Cloud Security & Threat

Introduction

Cloud Computing is basically an outsourced multi-tenanted IT Service model. The security concerns & threats applicable to cloud computing environment are same as applicable to any other IT environment. Only significant difference is that in the Cloud environment organizations lose control over the security measures required to protect their data and Information assets.

In a Cloud environment the responsibility of securing and maintaining a threat free environment lies partially with the customers and mainly with the service providers. However, the extent of responsibility depends upon the Cloud architecture & service model.

- SaaS - The service provider is responsible for the most of the security controls as the application & underlying platform including the infrastructure belongs to and is managed by the service provider.
- PaaS - Since the customer is deploying its application in service provider's environment, the



customer is responsible for the security controls around its application. The platform & underlining infrastructure is the service provider's responsibility.

- IaaS – The control in this case lies partially with the service provider and primarily with the customer as the customer has the privilege of configuring & managing part of the leased infrastructure.

Having said all of the above the customer using the cloud computing service would be accountable for its own information & data. For example a credit card company using cloud computing services of a service provider would still be responsible & accountable for its customer's personal information. The stack holders & customers would hold the credit card company responsible for any security breach.

So, it's very important that before going in for any cloud computing service the customers clearly understand the risks involved and the fact that they cannot do away with the accountability even if the responsibility of securing the information was that of the service provider.

Cloud Computing Threats

1. Unauthorized Access
2. Malicious Insiders
3. Abuse of CC Services
4. Inherent Vulnerabilities
5. Data Leakage
6. Espionage, loss of reputation
7. Legal & regulatory requirements
8. Unavailability of service

1. Malicious Insider:

As we all know internal threat is the major threat to Information Security. The situation is further exacerbating in the

Cloud Computing environment where the dependency is on the external service provider. There is no transparency in terms of how the vendor takes care of internal processes. For example there would be no clarity as to how the access is granted, access revocation, access review mechanisms etc. Also, there is no clarity on the service provider's recruitment process.

This opens the avenue for malicious insiders, disgruntled & disinterested employees which could lead to compromise of valuable critical & confidential information.

Impact:

Human risk is the worst of all specially in the cloud computing environment where there is no control on the people handling & managing your data. A malicious insider could lead to compromise of confidentiality, availability & integrity which are the pillars of Information Security. This could further lead to legal and regulatory implications.

Work Around:

- The policies, processes & controls defined by Cloud Computing service providers to protect against the threat of Malicious Insiders should be in line with the requirements or policies of their clients.
- Human resource requirements (Background verifications, Hire policies etc.) should be made part of Contracts with Service provider
- Clients should have transparency and right to audit / review service providers Information Security policy & processes
- Clients should include security breach clauses in the contracts
- Access should be granted on need to know basis. Service provider employee's

should be given access to only the resources that they are working on and access should be just enough for them to perform their job responsibilities

- Access logging & monitoring should be done

2. Unauthorized Access

Unauthorized access could be by external attackers or malicious insiders. The weak access, authentication & authorization controls could lead to unauthorized access. Depending upon the type of Cloud Computing service, the clients / customers might have limited or no say in defining the controls to prevent unauthorized access. For example in SaaS model the clients have a very limited option in defining the access controls. While in PaaS at least the application level access controls can be defined by the clients.

Impact:

Unauthorized access could lead to compromise of confidential & critical information. This could have legal and regulatory implications as well.

Work Around:

- Service provider should define a strong Information Security (IS) Policy & enforce adherence to the IS policy and procedures
- Clients should have transparency and right to audit / review service providers Information Security policy & processes
- Security breach clauses could be possibly included in the contracts with the service providers

3. Inherent Vulnerabilities

Applications and Infrastructure devices have inherent vulnerabilities which if not taken care of could lead to compromise of

CIA. Applications are vulnerable to SQL Injections, XSS, Session Hijacking, malicious file upload etc. Similarly servers & network devices are vulnerable to unauthorized access, DoS, buffer overflows etc. Once again the responsibility of taking care of the vulnerabilities & security holes depends upon the Cloud Computing service model. In case of PaaS if the customer is responsible for the application being hosted in the service provider facility; while service provider is responsible for the platform and underlining infrastructure. In SaaS the service provider has greater or almost the entire responsibility of ensuring a secured service.

Impact:

The application vulnerabilities like SQL Injection could result in compromise of client data stored in database. Vulnerabilities like XSS and Session Hijacking could lead to unauthorized access, installation of malwares / backdoors etc. Similarly vulnerabilities in the infrastructure components could lead to compromise of customer's information, data leakage, DoS etc.

Exploitation of vulnerabilities could also have legal & regulatory concerns for the customers due to data leakage, unavailability of service etc.

Work Around:

- Service provider should ensure that the application and infrastructure vulnerabilities are identified and fixed
- Patches and fixes should be applied on regular basis
- Security audits should be conducted on periodic basis and appropriate measures should be taken to fix the identified bugs
- Customers should have rights to review the security audit reports

- Depending upon the criticality of information in Cloud Computing environment the customers should have rights to conduct a security review of service provider applications and infrastructure
- Customers should also look into the best practices / guidelines / certifications followed by the service providers like ISO 27001, TIA 942 etc.

4. Data Loss / Leakage

Data could be leaked through many possible ways. Some of the causes could be malicious insiders, sharing of data between employees, improper & irregular backups, inappropriate data retention policy, users forgetting the secret keys / passwords etc. Once again data leakage risk is aggravated in a Cloud Computing environment because the ownership is yours however the control on processing & storing the data is not in your hands.

Impact:

Depending upon the cloud model & criticality of data being processed & stored in cloud Data Loss / Leakage could have some serious fall outs. Apart from loss of confidentiality, reputation for the customer's data leakage could also possibly have legal repercussions as well. Further to make the matters worse loss of intellectual property could cause competitive and financial grievances to the customers.

Work Around:

- As much as possible the information & data sensitive in nature should not be stored with a service provider.
- Customers should ensure that service providers should provide services as per the Information Security policy & procedures of customers. This would

provide some level of comfort and control to prevent data leakage / loss

- Customer should define or should lay down in the requirement list as to how their data should be accessed, handled, processed and backed up. These requirements should be taken into consideration while drafting the contracts & SLA's with the service providers. .

5. Espionage & Loss of Reputation

In today's highly competitive and fast pace world competitor espionage is a growing threat. The loss of confidential and intellectual property due to espionage can lead to loss of business, reputation, good will, shareholder's trust etc. In a cloud computing scenario attackers and nefarious users could possibly take advantage of the fact that the proprietary and confidential data is stored with an outsider which could be leveraged to cause damage to the reputation of the parent organization.

Impact:

Espionage can lead to loss of business, loss of reputation, loss of good will etc. Any leak of confidential information can also have legal and regulatory implications.

Work Around:

- Strong Information Security (IS) Policy, Procedures & Process should be defined by Cloud Computing vendors
- Cloud computing service providers should also implement strong Security controls around the applications & IT infrastructure
- The Operational efficiency of security controls should be reviewed periodically
- The IS policy & Security controls should be reviewed and updated to counteract the ever increasing security threat

- Customers should have transparency in the Security measures adopted by the Cloud Computing vendors

6. Legal & Regulatory Requirements

We are so much surrounded by legal & regulatory requirements like SOX, SAS 70, HIPAA, PCI DSS etc. Depending upon the nature of business and kind of data being handled different legal & regulatory requirements are applicable. In Cloud Computing scenario it becomes imperative that the service provider should meet the legal & regulatory requirement on behalf of the customers. So if a Cloud Computing service provider is servicing a client in Health Care sector then it should take care of HIPAA requirements. Similarly service provider providing Cloud Computing services to Credit Card Company should take care of the PCI DSS requirements. It becomes the customers responsibility to ensure that in spite of using the Cloud Computing services their legal & regulatory requirements are being met.

Implications:

Not meeting the legal & regulatory requirements could lead to legal actions causing loss of business, public trust, financial penalties and imprisonment as applicable.

Work Around:

- Customers / clients should have a very good understanding of the legal & regulatory requirements applicable to their business
- Customers should ensure that their legal & regulatory requirements are being fulfilled even in the Cloud Computing scenario
- Service provider should also have a clear understanding of the legal & regulatory

requirements of their clients before offering their services.

- Service provider should make necessary provisions to ensure that the legal & regulatory requirements of their clients are being met.
- Customers should have transparency into the certifications & processes being followed by the service providers to ensure that the legal & regulatory requirements are met

7. Unavailability of Service

Today we all need 24x7 access to our data (official or personal). Many businesses like Banks & Military Operations rely on real time information and need to have 0 down time. Unavailability of information can have direct financial, legal & security implications. The processes and technologies are designed to ensure that information is available at all times and in case of problems downtime is within acceptable limits. Unavailability of service can be due to many reasons like inadequate backups, no BCP / DR, unavailability of resources etc.

In a Cloud Computing environment service provider is responsible for the availability of service and maintaining an acceptable downtime based on the clients requirements.

Implications:

Availability is one of the pillars of CIA. Unavailability of information in critical services like military operations can be a threat to National Security and in banking operations unavailability of information can have direct financial implications. In today's complex and data availability driven world it is very imperative that information is available most of the times and unavailability is within the acceptable limits.

Work Around:

- Customers should define well-structured and all-encompassing SLA's with cloud computing service provider's to ensure the availability of their data
- Based on criticality of information being processed or stored with service providers considerations for Backup, BCP / DR should be taken into account
- Customers should evaluate the potential of the service provider to meet the availability requirements. For example if the service provider has enough human staffing, alternate DR Site availability, backup facilities etc.
- Customers should have transparency in the measures taken by the service provider to ensure availability

8. Abuse of CC Services:

Many a times the Cloud Computing service providers do not have strict registration process. Using a credit card any one can register for cloud computing services online or many vendors offer free trial of their services. This opens an avenue for many nefarious users, who could anonymously exploit the cloud computing resources for malicious purpose like setting up botnets, spamming, spreading virus / malwares etc. The attackers could attempt DoS, exploiting the known vulnerabilities, etc. to compromise the cloud computing resources which would lead to compromise of other customer's resources hosted in the same environment. For example an online cloud based corporate email service & web portal might be vulnerable to SQL injection & XSS which when exploited could result in compromise of other corporate's information / email hosted in the same environment.

Implications:

- Spread of virus, malwares , spam emails, loss of confidentiality etc.,
- Cloud computing environment used as botnets to launch further attacks

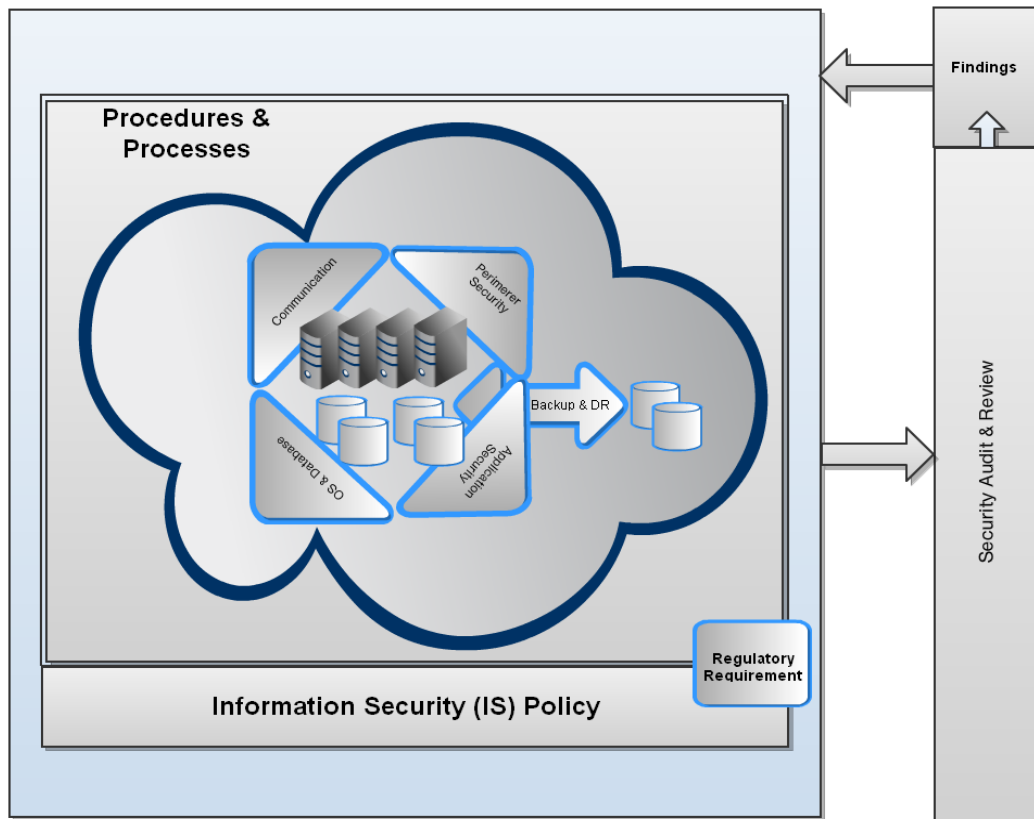
Work Around:

- Service provider should have stricter and regulated registration process
- Monitor the customer traffic for any malicious or nefarious activities

Periodic security assessment to ensure that the service provider's own network and other resources are not infested or compromised

Cloud Computing Security Framework

1. Information Security Policy
2. Regulatory requirements
3. Procedures & Processes
4. Backups & DRP
5. Communication Security
6. Perimeter Security
7. IT & Application Security
8. Security Audit & Reviews



1. Information Security (IS) Policy:

IS Policy is the starting point and most critical component in protecting the Information asset of any organization. The IS Policy needs to define the CIA requirements and how the same can be achieved. IS Policy is a High Level framework addressing everything related to protecting the Information Assets as per the organization's functioning and operations. IS Policy is organization wide and is applicable to all of the organization and its subsidiaries. Subsidiaries can have their own IS Policy which in a way would be subset of the parent entity IS Policy.

In a Cloud Computing environment it is imperative that the service provider defines a stringent and all-encompassing IS Policy which ideally meets the requirements of all its customers and their respective Information Security requirements. Without a holistic and structured IS Policy the procedures followed and technology used to protect Information assets will never be

adequate. Also as technology matures and new vulnerabilities & security holes are discovered, IS Policy needs to be updated on an ongoing basis.

Amongst others IS Policy takes care of the following:

- Physical & Logical Access control requirements
- Encryption requirements & techniques
- Program changes & version management
- Backup & Retentions
- BCP & DRP requirements
- Incidence Response
- Regulatory requirements
- Security reviews / audits
- Patches / Updates / AV Solutions / plugging security holes

2. Regulatory requirements:

Service provider should understand the regulatory requirements of its clients. In a Cloud Computing environment since the

customers would be using the service provider resources or in many cases storing their data with service provider; it becomes service provider's responsibility to understand and meet the regulatory requirements on behalf of their customers.

Based on the requirements service provider should be able to meet requirements of SOX, SAS70, HIPAA, PCI – DSS, SAS 70, ISO27001 etc. Some of the regulatory requirement restricts storing of data outside the country. The customers should be aware of such requirements and should clarify with the service provider & ensure that their data would not be stored in locations which not permitted.

The customers before getting in a contract with a Cloud Computing service provider should ensure that the service provider meets their regulatory requirements. It also gives an added level of comfort and sense of security to know if service providers follow or meet certain standards for e.g. their DataCenter is as per TIA 942 requirements, the service provider is ISO 27001 certified etc.

3. Procedures & Processes:

The IS Policy lays a very high level guidelines to be followed throughout the organization to ensure Information & Data security. Procedures & Processes are defined in line with the IS Policy to ensure that the requirements defined in the Policy are met. The group companies / subsidiaries & individual departments can define their own procedures and processes based on the IS Policy requirements. For example IS Policy might mention strong access control requirements and based on this requirement physical access control for data center would have 2 factor authentication (biometrics & access card) while a HR

department can only have one level of authentication (access card).

In a Cloud scenario it is quite critical that service providers have a well-defined & holistic Procedures & Processes based on the IS Policy. All the aspects of IS Policy should be taken into account. Ideally procedures & processes should address the requirements of all the clients. It is service provider's responsibility to ensure that defined procedures & process are strictly followed, deviation if any or noted and acted upon. Customer / clients should have rights to audit / review the Policy & procedures defined and followed by the service provider.

4. Backups & DRP:

Data availability is one of the biggest concerns in a Cloud Computing environment. Service provider should ensure that data availability requirements of respective clients are met. Data should be backed up and retained as per the defined IS Policy & procedures. Service provider should also do a periodic restoration drills to ensure that the backed up data is available in required time frame.

Service provider should also define a Business Continuity & Disaster Recovery Plan (BCP & DRP) as per the need of the clients. Some clients like Financial sector might need 24x7 availability with 0 downtime while some others might have x number of hours as acceptable downtime. So the service provider should provide the clients with options as per their requirements. Also, provision should be made available for various DR site options (cold, warm, and hot). Regular DR drills should be conducted to ensure that the resources & facility is available in case of an actual disaster.

Customers should review the Backup procedures and BCP – DRP of the service

providers and if need be conduct audits to ensure that it meets their data availability requirements.

5. Communication Security:

It is very important to ensure that the channel used to connect to service provider or its resources is secured. SSL, VPN, SFTP and other end to end encryption techniques should be used. In a Cloud Computing environment service provider should ensure that the applications and services designed should meet the security requirements. For example HTTPS should be used instead of HTTP; SFTP should be used instead of FTP. Communication security becomes more critical the Cloud Computing scenario where the data resides in a multi-tenant shared infrastructure and it has accessed in most of the instances thru insecure public internet.

6. Perimeter Security:

Perimeter security is basically building a strong physical & logical fortress to prevent intruders & attackers. The physical premises of the service provider should be well guarded. The access should be granted on need to know basis. All the entry and exit points should be secured to prevent unauthorized access. In a Cloud Computing scenario where critical data of multiple customers is being processed any unauthorized physical access can lead to compromise of confidentiality of the information which in return can have severe legal & regulatory implications.

Appropriate devices like Firewall, IPS / IDS should be put in place to take care of the logical perimeter security aspect.

7. IT & Application Security:

The applications, underlining OS & database should be free of vulnerabilities and security holes. The customers rely on Cloud service providers for providing a secured & risk free service. Hardening Policy / Baseline should be defined to address the security requirements of IT Infrastructure. Before an OS or database is deployed in production it should be hardened as per the hardening guidelines and a thorough security assessment of the same should be conducted. Same treatment is applicable to the applications being deployed in the cloud environment. The process of hardening is applicable to virtual environment as much it is applicable to the real infrastructure.

8. Security Audit & Reviews:

With the nature of business in Cloud it is necessary that a Security Review / Audits are conducted periodically. The review should start with the review of the IS Policy and underlining processes & procedures. It should be ensured that the defined processes are as per the IS Policy requirements. The processes should not only be defined but also should be followed and exceptions if any should be noted and duly authorized. In case of Cloud Computing with multiple customers relying on service provider there is very little margin or rather no margin for deviations and exceptions.

The Security Review / Audit should also include Security Assessment of IT Infrastructure & Applications to ensure that they are secured against vulnerabilities & security holes. In today's technology driven world everyday new vulnerabilities are discovered and appropriate work around and patches are developed by the vendors. It should be ensured that these vulnerabilities are plugged and the systems are patched. As an outcome of Security Review, if need be IS

Policy & underlining procedures like Baselines / Hardening documents should be updated to meet the security requirements and prevent compromise of the Information Assets.

Some of the Cloud Computing Security Breaches

Unauthorized Access to data in the Cloud:

Twitter employee's email ID was compromised leading to unauthorized access to corporate information stored on Google Apps. This was a clear example of Privacy concerns looming in the Cloud Computing environment.

Details:

http://www.computerworld.com/s/article/9135893/Twitter_breach_revives_security_issues_with_cloud_computing

DoS in the Cloud

In a proof of concept (PoC) exercise researchers were able to bring down a small company using Cloud services off the internet. The researchers registered as legitimate users for Amazon's EC2 service and conducted targeted attacks on their client's network to cause a complete Denial of Service.

Details:

<http://www.darkreading.com/smb-security/security/perimeter/showArticle.jhtml?articleID=226500300>

Social Engineering attack

Back in 2007 there was a Social Engineering attack on a salesforce.com employee leading to possible phishing attacks on the salesforce.com employees & its customers.

In a Cloud Computing environment a phishing scam could lead to compromise of confidential details possibly causing financial & personal grievances.

Details:

<http://www.zdnet.com/blog/berlind/phishing-based-breach-of-salesforcecom-customer-data-is-more-evidence-of-industrys-need-to-act-on-spam-now/880>



Vishal Kalro

Information Security Consultant with KPMG. Specializing in Infrastructure & Network Security. BE - Electronics, ME - Telecommunication.
<http://twitter.com/awish11>



Amit Parekh

Amit works as Asst. manager with KPMG India, and has background in Security Consultancy and Security Research. His core areas of expertise are Application Security, Network Security and Source Code reviews. He is an avid gamer and reader and takes interest in malware analysis and reverse engineering.



Deep Packet Analysis on Cloud

Introduction

As we are discussing all about cloud in this issue we'd love to see a few tools on the cloud itself.

The most interesting work for any security professional is to analyze the packet captures. Our friendly .pcap files. PCAP files can be generated from your favorite tools like TCPDump or Wireshark.

Let's see two ways to understand and do deep packet analysis on the cloud itself

PCAPR

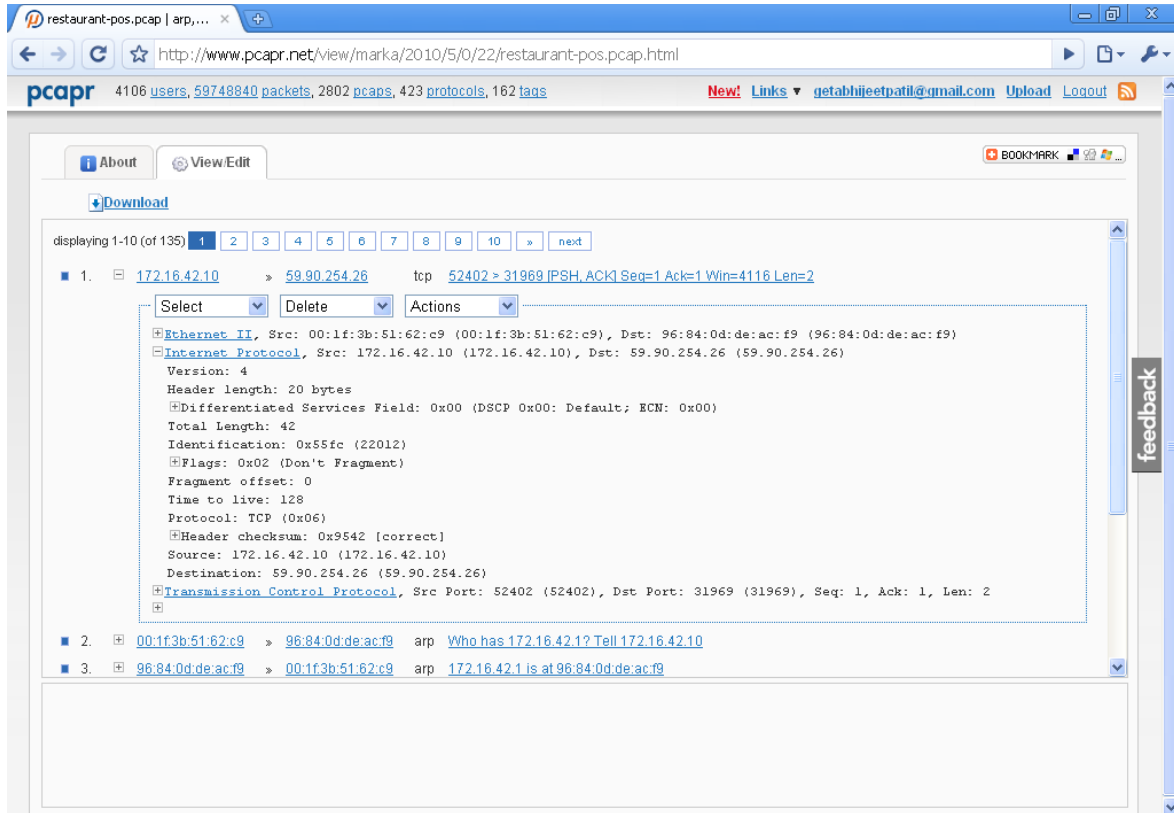
<http://pcapr.net> is a social networking site, where 'friends' can learn and teach about pcaps to each other.

It's a web service where you can upload your pcap files and study the packets inside the pcap file.

As a drawback you can upload only 4048kb files limiting to 500 packets per file. Check out <http://pcapr.net/faq> for other details.

PCAPR project has another cloud based tool called XTRACTR
<http://www.pcapr.net/xtractr>

xtractr is a hybrid cloud application for indexing, searching, reporting, extracting and collaborating on pcaps. This enables you to rapidly identify field issues and perform network forensics and troubleshooting with just a few clicks. The lite version of xtractr can index up to 10 million packets or 1 Gbyte of pcaps.



Cloudshark

Now the question arises that if we have our own favorite Wireshark & have to use it for pcap generation why can't we use it only & why not something similar in interface.

The point of having such a tool online is that you can actually generate pcap from anywhere and upload it for future reference. And as far as UI is concerned, let's look at cloud shark. <http://cloudshark.org/>

As per Cloud Shark

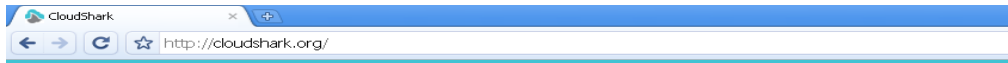
We work with network capture files on a daily basis. After trying to view capture files on mobile devices without Wireshark support, we realized it was time to move packets to the cloud. The CloudShark idea was born. CloudShark was created to

Make viewing capture files easy from any device ranging from desktops to smart phones. After creating our own solution, we decided to make it available to everyone as CloudShark.org.

Interface of CloudShark is similar to your favorite Wireshark and you can view/analyze packets the same way as you would do on Wireshark.

Working with CloudShark is simple.

- Generate your capture file or use an existing capture file
- Email it, upload it, or link it
- CloudShark does the rest by providing a decode session
- If you email CloudShark with an attached capture file, we'll email you



CloudShark brings your network capture files to the web. Import, view, and share your capture files from anywhere with a web browser.

Start using CloudShark now! There are no sign-ups or logins needed.

1. [Upload a File](#)
2. [Import from a URL](#)
3. Email it to cap@cloudshark.org

Any Questions? Check out an [example](#), learn more from the [FAQ](#), or visit us on [the beach!](#)

back with a link to your decode session

- Send your capture files as an attachment to cap@cloudshark.org
- If you are in the browser already, we'll drop you into your decode session

But the limitation of packet capture size holds well on CloudShark also. Here you are allowed to view first 2500 packets only.



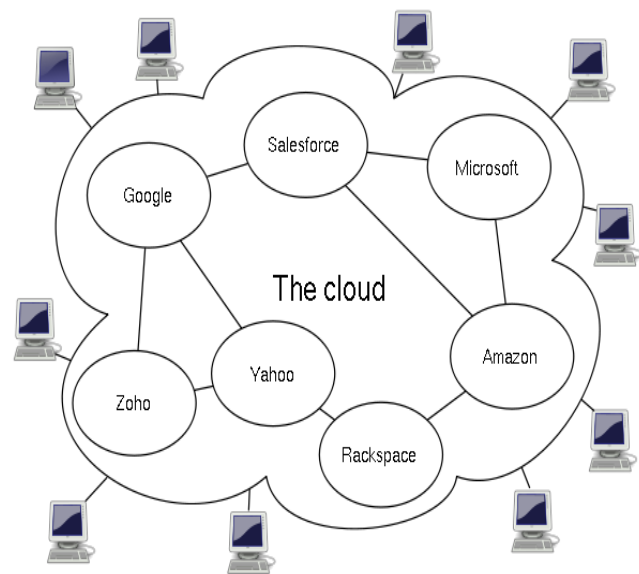
Varun Hirve
varun@chmag.in



What the heck is Cloud Computing?

What is Cloud Computing?

Cloud Computing is the next big thing in Internet's revolution. The "Cloud" represents "Internet" and "Cloud Computing" means "Internet Computing". According to Wikipedia, Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid.



In cloud computing you can use the pool of computing resources available like storage, applications, servers, services, and information etc. on pay-as-you-use basis.

Since all the resources are available on the web, you need not invest your valuable time, money and efforts in hardware resources.

This increases agility, reliability, scalability and helps in reducing cost, maintenance efforts. Let's have a look at cloud computing in more detail.

Characteristics of Cloud Computing

1. **On-demand self-service:** User can request and configure services by themselves without requiring much help from service providers.
2. **Broad network Access:** Services are available on all the Internet-enabled devices like desktops, laptops, PDAs, mobile phones etc.
3. **Resource Pooling:** The service providers give shared access to computing power spread across multiple geographic locations – multi-tenancy
4. **Rapid elasticity:** Elasticity can be defined as the ability to scale up or back depending on demand of resources. In cloud computing Customers can increase or decrease the demand of resources at will.
5. **Measured service:** Customers pay only for the resources they have used. This billing system is based to the pay-as-per-use model.

customize the application. He does not control or manage the underlying hardware or network infrastructure.

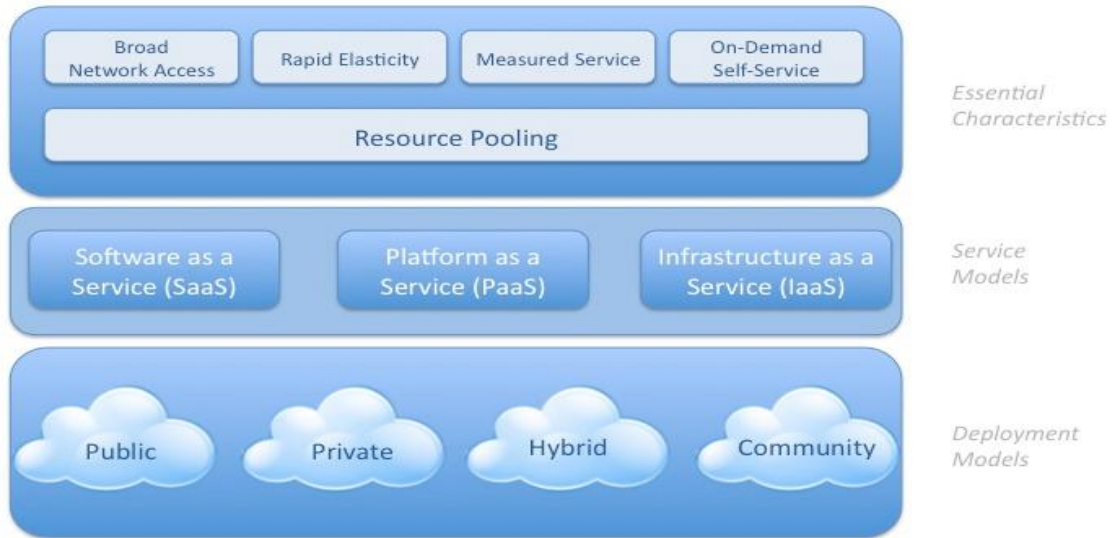
3. **Cloud Infrastructure as a service (IaaS):** Customers are provided with the storage, networking and other fundamental computing resources. Here customer can deploy their operating systems and applications. They have control on the operating system, applications and storage and may also have limited control on networking infrastructure like firewalls etc.

Cloud Service Models

There are three types of cloud service models – Software, Infrastructure and Platform.

1. **Cloud Software as a Service (SaaS):** The service providers provide customers the access to the software(s) already installed on the cloud. Customers don't need to install or manage or buy any hardware for the software. He just has to connect it and use it. Customer controls only the application and not they underlying operating system, hardware or network infrastructure.
2. **Cloud Platform as a Service (PaaS):** Customers are provided with operating system layer and application toolset. Customer controls the application and can also

Visual Model Of NIST Working Definition Of Cloud Computing
<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



Cloud Deployment Models

There are four types of deployment models irrespective of service models:

- 1. Public Cloud:** The cloud infrastructure is owned by cloud service provider and is made available to general public or some large organization.
- 2. Private Cloud:** The cloud infrastructure is owned or leased by a single organization and is operated by the organization only.
- 3. Community Cloud:** The cloud infrastructure is owned and managed by a group of organizations who have shared interest like security requirements, policies or common mission.
- 4. Hybrid Cloud:** The cloud infrastructure comprises of two or more models (public, community or private).

Note: Private clouds are known as internal clouds and Public clouds are called as External Clouds.



Abhijeet Patil
Abhijeet@chmag.in



CLOUD AND LAW

The major legal challenge emerging from cloud computing is the issue of extradition and jurisdiction. To understand the extent and jurisdiction of the Information Technology Act, we must examine sections 1(2) and 75 of the Act.

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

75. Act to apply for offence or contravention committed outside India.

- (1) Subject to the provision of subsection (2), the provisions of this
- (2) Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
- (2) For the purposes of subsection(1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Not only does the Information Technology Act apply to the whole of India, but also to contraventions committed outside India, by anyone, involving a computer located in India.

Illustration: Kylie Minogue, an Australian national, residing in USA, gains unauthorized access to a computer located in India and

deletes information. In this case, she will be liable under the provisions of the IT Act.

However, there are exceptions to the term “any person”. Certain persons are exempt from prosecution under the IT Act. These include the President of India and the Governors of Indian states¹, Foreign Heads of State and Ambassadors of foreign countries².

Extradition is the delivery of a person accused of a crime in one country by the other country where he has sought refuge.

Illustration:

Sameer has committed a crime in India and then escaped to USA. The US government could extradite Sameer to India so that he can face trial for his crime.

¹ Article 361(2) of the Constitution of India states that “No criminal proceedings whatsoever shall be instituted or continued against the President, or the Governor of a State, in any court during his term of office.” Article 361(3) states “No process for the arrest or imprisonment of the President, or the Governor of a State, shall issue from any court during his term of office.”

² The principle of diplomatic immunity is enshrined in the “Vienna Convention on Diplomatic Relations” of 1961. The **convention** mentions that “the purpose of such privileges and immunities is not to benefit individuals but to ensure the efficient performance of the functions of diplomatic missions as representing States”. This has been codified in India under the Diplomatic Relations (Vienna Convention) Act, 1972. Similar immunities are conferred on United Nations officers by the United Nations (Privileges and Immunities) Act, 1947.

The delivery takes place pursuant to an existing treaty or an ad hoc arrangement. Extradition is based on the broad principle that it is in the interest of civilized communities that crimes should not go unpunished.

The domestic law of the nation from whom the extradition of the person is sought plays a crucial role in determining whether the State seeking the extradition would be granted its request or not. Extradition Act, 1962 is the relevant law in India.

India has entered into extradition treaties with Belgium(1958), Bhutan (1997), Canada (1987), Hong Kong 1997), Nepal(old Treaty) (1963), Netherlands (1989), Russia (2000), Switzerland (1996), UAE (2000), U.K. (1993), USA (1999), Uzbekistan (2002), Spain (2003), Mongolia (2004), Turkey (2003), Germany (2004), Tunisia (2004), Oman (2005), France (2005), Poland (2005), Korea(ROK) (2004), Bahrain (2005), Bulgaria (2006), Ukraine (2006), South Africa (2005), Belarus (2008), Kuwait (2007) and Mauritius (2008). Additionally India has extradition agreements with Australia (1971), Fiji (1979), Italy (2003), Papua New Guinea (1978), Singapore (1972), Sri Lanka (1978), Sweden (1963), Tanzania (1966), Thailand (1982) and Portugal (2002).



Rohas Nagpal
rn@asianlaws.org

Command LINE



Command line access to Cloud Services

Introduction

Now we have decided that everything in this issue will be discussed on cloud only. Although this individual article might not be that great for help but let's explore how we can use command line tools to upload our content on Amazon AWS and Google App Engine

Amazon EC2 & S3

S3cmd <http://s3tools.org/s3cmd> is a command line tool for uploading, retrieving and managing data in Amazon S3. It is best suited for power users who don't fear

command line. It is also ideal for scripts, automated backups triggered from cron, etc.

S3cmd is an open source project available under GNU Public License v2 (GPLv2) and is free for both commercial and private use. You will only have to pay Amazon for using their storage.

Though this is not the only tool but I prefer using the same for my activity and hence it would be easier for me to write the same. The HOWTO guide on the website is sufficient enough to understand and play around. Some excerpts are here.

Download

```
svn co
https://s3tools.svn.sourceforge.net/svnroot/s3tools/s3cmd/trunk/
```

Or simply go to <http://s3tools.org/download>

Configure

```
s3cmd --configure
```

You will be asked for the two keys - copy and paste them from your confirmation email or from your Amazon account page. Be careful when copying them! They are case sensitive and must be entered accurately or you'll keep getting errors about invalid signatures or similar.

There's an option to decide about use HTTPS or HTTP transport for communication with Amazon. HTTPS is an encrypted version of HTTP, protecting your data against eavesdroppers while they're in transit to and from Amazon S3.

List all buckets.

```
s3cmd ls
```

Make a bucket

```
s3cmd mb s3://my-bucket-name
```

List content of a bucket

```
s3cmd ls s3://my-mucket-name
```

Upload a file in a bucket

```
s3cmd put file.ext s3://my-bucket-name/file.ext
```

Retrieve a file from bucket

```
s3cmd get s3://my-bucket-name/file.ext file.ext
```

Delete a file from bucket

```
s3cmd del s3://my-bucket-name/file.ext
```

Remove a bucket

```
s3cmd rb s3://my-bucket-name
```

Remember, a bucket will not be deleted unless it's empty

Google App Engine

Google App Engine supports the command line upload/update of content using python.

Creating a local site and configuration file:

Create a local folder on your machine for this project. Put a folder inside that containing all your web pages. It can be called anything, but the AppEngine examples always call it **static**. For the sake of our article let's call it **home**

Say if your project folder is at **C:\MyWeb** then this folder will be **C:\MyWeb\home**, and the main home page would probably be **C:\MyWeb\home\index.html**. So now you have a local folder on your machine @ **C:\MyWeb\home** which holds your application.

Now create a text file called **app.yaml** in the project folder

(**C:\MyWeb\app.yaml**) with the following contents (I hope you know that you have to changethemysamplesite entry to the name you registered):

```
application: mysamplesite
version: 1
runtime: python
api_version: 1
handlers:

- url: (.*)/
  static_files: home\1/index.html
  upload:
    home/index.html

- url: /
  static_dir: home
```

Creating the environment for upload:

The website and all related configuration is now ready for upload. Now you need to set up the environment for it. Don't worry I'll not ask you to do any coding, it's simple "next-> next" kind of installation

Download and install python from <http://www.python.org/download/> and install it. (Simple "next->next" installation)

Download and install Google AppEngine SDK from <http://code.google.com/appengine/downloads.html> (Nothing to worry I promise)

Uploading the website:

Now it's the time to upload your static website. All you have to do is run the following command from command prompt.

appcfg.py update C:\MyWeb

Appcfg.py will come from Google App Engine SDK. This will ask you for your email address. Enter the one you used for creation of application. Next it will ask for your Gmail password, don't worry & type it too.

It will show some text and screen & BANG! your web application is up and running on Google AppEngine.

Now you can access your website by the url <http://mysamplesite.appspot.com/> (change ***mysamplesite*** to your project name).



Rohit Srivastwa
rohit@clubhack.com



ITS THERE, UP IN THE CLOUDS

WHERE THE HECK IS MY DATA

@pankit_thakkar