 ISBN: 978-81-931039-3-7

SURVEY PAPER ON CLOUD COMPUTING

Kalpana Tiwari[1], Er. Sachin Chaudhary[2], Er. Kumar Shanu[3]

[1,2,3] *Department of Computer Science and Engineering*

Bhagwant Institute of Technology, Muzaffarnagar, Uttar Pradesh (India)

ABSTRACT

Cloud computing is an attractive computing model as it allows for resources to be provisioned according on a demand basis. Cloud uses open source operating system like Ubuntu 10.04 server addition. It replaces traditional software installations, licensing issues into complete on-demand services through Internet.

I INTRODUCTION

Cloud Computing is a model which is found everywhere; it is convenient, on demand network access to a shared pool of configuration computing resource .Example Network server, storage application & service provider interactions. For example on facebook a social networking website users upload videos which uses cloud providers storage service so less hardware cost for clients [1].

There are three types of cloud computing models: Public cloud, Private cloud & Hybrid cloud. In public cloud, the resources are provided over internet to all the clients. In Private cloud, resources are provided over intranet within an organization. Hybrid cloud is a provision depending on requirement can provide resources within an organization or publicly.

II SERVICE MODEL CLASSIFICATION

Depending on the service models [2] , clouds are classified as:

1. Software as a Service (SaaS): In this model the user purchases the ability to use a software application or service on the cloud. Example Google Docs
2. Platform as a Service (PaaS):In this model the user purchases access to platforms, enabling them to deploy their own applications on the cloud. .Example Google App Engine
3. Infrastructure as a Service (IaaS): In this model, the user is delivered infrastructure, namely servers, networks and storage. The user can deploy several Virtual Machines and run specific Operating System on them. .Example Amazon EC23, Windows Azure etc.

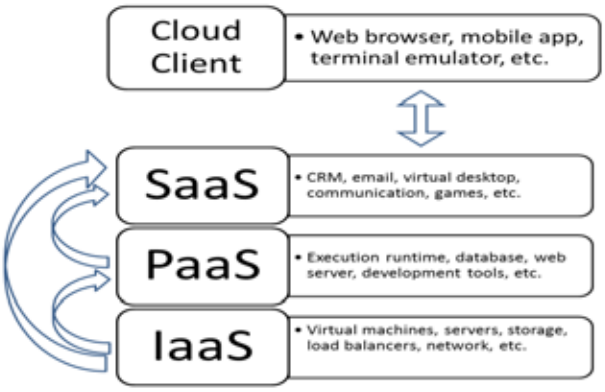


Fig.1 Service Models

III EUCALYPTUS ARCHITECTURE

It is an open source cloud computing framework focused on academic research. It provides resources for experimental instrumentation and study. Eucalyptus users are able to start, control, access and terminate entire virtual machines. In its current version, Eucalyptus supports VMs that run atop the Xen supervisor [3].

The Eucalyptus project four characteristics that differentiate it from others cloud computing solutions:

a) Eucalyptus was designed to be simple without requiring dedicated resources;

b) Eucalyptus was designed to encourage third-party extensions through modular software framework and language-agnostic communication mechanisms;

c) Eucalyptus external interface is based on the Amazon API and

d) It provides a virtual network.

3.1 Eucalyptus is Comprised of Six Components

a. **Cloud Controller (CLC):** It is a java program that act as web interface to the outer world. The CLC acts as the administrative interface for the cloud, querying the other components about resource availability and performing high level resource scheduling by making requests to the Cluster Controller (CC). The CLC can be accessed through command line interfaces like euca2ools to manage storage and network resources. Only one CLC can exist per cloud and it handles all authentication, accounting, reporting etc [4].

b. **Walrus:** Walrus is a java program which is Eucalyptus equivalent of the AWS Simple Storage. Walrus offers users the ability to store persistent data, organized as buckets and objects, to all the virtual machines and can be used as a simple HTTP put/get storage as a service solution. There are no particular data type restrictions. Users can store application data as well as the images which are the building blocks used to launch the VMs. Volume snapshots, which are point in time copies of data, can also be stored on Walrus.

c. **Cluster Controller**: Cluster Controller is written in C and acts as the front end of a particular cluster within the Eucalyptus Cloud. It executes on a machine that has connectivity to both the CLC and the Node Controllers (NC) and reports the NCs registered to the CLC.CC also gather the information about a set NCs and schedules the VM execution on specific NCs. The CC also manages the virtual machine networks and all NCs within a single CC will belong to a single subnet.

d. **Storage Controller:** Storage Controller, written in Java, is the Eucalyptus equivalent of the Amazon's Elastic Block Storage. It can interface with various types of storage systems. It communicates with the Cluster Controller and Node Controller and manages the Eucalyptus block volumes and snapshots to the instances within its specific cluster. EBS volumes persist even after VM termination but cannot be shared between VMs and can only be accessed within the same availability zone in which the VM is running.

e. **Node Controller:** The Node Controller (NC) is written in C and it runs on the machine that hosts the VM instances. It runs on each node and interacts with the CC on one hand and the OS and the hypervisor on the other side. It controls VM activities like the execution, inspection and termination of VM instances. It downloads and creates caches of images and snapshots from the Walrus. It is also responsible for the management of the virtual network endpoint. There is no theoretical limit to the number of NCs per cluster but performance limits do exist.

3.2 Benefits of Eucalyptus

1. Eucalyptus has a modular and easy design which enables a variety of user interfaces and thus brings the benefits of virtualization to a broad spectrum of users like administrators, developers, managers and hosting customers.

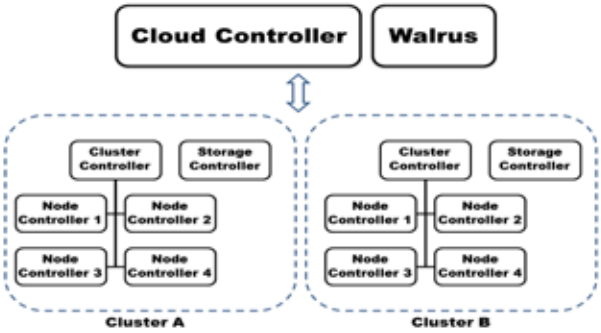


Fig.2 Eucalyptus architecture

2. The snapshot feature provides opportunities to improve the reliability and automation of the cloud making it very easy to use and reduce average learning time for users, thus improving turnaround time for projects.
3. Supports existing virtualization technologies, Linux-based operating systems, and supports multiple hypervisors.
4. Since the core of the Eucalyptus project will continue to remain open-source, users can access the different resources at different place.

3.3 Eucalyptus Framework Setup

SYSTEM REQUIREMENTS

1. Compute Requirements:

1. Physical Machines: All Eucalyptus components must be installed on physical machines, not virtual machines [5].

2. **Central Processing Units (CPUs):** It is recommended that each machine in your Eucalyptus cloud contain either an Intel or AMD processor with a minimum of two, 2GHz cores.
3. **Operating Systems**: Eucalyptus supports Ubuntu 12.04 LTS and some other Linux distributions.
4. **Machine Clocks**: Each Eucalyptus component machine and any client machine clocks must be synchronized (for example, using NTP) at all the time, not just at installation.
5. **Hypervisor:** Ubuntu 12.04 LTS installations must have KVM installed and configured on NC host machines. VMware-based installations do not include NCs, but must have a VMware hypervisor pool installed and configured.
6. **Machine Access:** Verify that all machines in your network allow root or pseudo access and SSH login.

STORAGE AND MEMORY REQUIREMENTS

The following are recommended:

1. Each machine in your network needs a minimum of 30 GB of storage.
2. At least 100 GB for Walrus and SC hosts running Linux VMs.
3. 50-100 GB per NC host running Linux VMs.
4. Each machine in your network should have at least 4 GB RAM or above for improved caching.

3.4 Network Requirements

1. All NCs must have access to a minimum of 1 GB Ethernet network connectivity [6].
2. All Eucalyptus components must have at least one Network Interface Card (NIC) for a base-line deployment. For better network isolation and scale, the CC should have two NICs each with a minimum of 1 GB Ethernet (one facing the CLC/user network and one facing the NC/VM network).
3. Depending on some configurations, Eucalyptus requires that you make available two sets of IP addresses. The first range is private, to be used only within the Eucalyptus system itself. The second range is public, to be routable to and from end-users and VM instances. Both sets must be unique to Eucalyptus, not in use by other components or applications within your network.

IV REGISTERING EUCALYPTUS

Eucalyptus implements a secure protocol for registering separate components. You only need to register components the first time Eucalyptus is started after it was installed.[6][7]

Most registration commands run on the CLC server. NCs, however, are registered on each CC. Note that each registration command will attempt an SSH as root to the remote physical host where the registering component is assumed to be running. The registration command also contacts the component so it must be running at the time of the command is issued.

NCs need only two pieces of information: component name and IP address. Other component requires four pieces of information:

1. The component (–register-XYZ) you are registering, because this affects where the commands must be executed.
2. The partition (–partition) the component will belong to. The partition is the same thing as availability zone in AWS.
3. The name (–component) ascribed to the component. This name is also used when reporting system state changes which require administrator attention. This name must be globally-unique with respect to other component registrations.
4. The IP address (–host) of the service being registered.

V FUNCTIONALITY

The Eucalyptus User Console provides an interface for users to self-service provision and configure compute, network, and storage resources. Development and test teams can manage virtual instances using built-in key management and encryption capabilities. Access to virtual instances is available using familiar SSH and RDP mechanisms. Virtual instances with application configuration can be stopped and restarted using encrypted boot from EBS capability [7].

IaaS service components Cloud Controller, Cluster Controller, Walrus, Storage Controller, and VMware Broker are configurable as redundant systems that are resilient to multiple types of failures. Management state of the cloud machine is preserved and reverted to normal operating conditions in the event of a hardware or software failure.

Eucalyptus can run multiple versions of Windows and Linux virtual machine images. Users can build a library of Eucalyptus Machine Images (EMIs) with application metadata that are decoupled from infrastructure details to allow them to run on Eucalyptus clouds. Amazon Machine Images are also compatible with Eucalyptus clouds. VMware Images and vApps can be converted to run on Eucalyptus clouds and AWS public clouds.

Eucalyptus user identity management can be integrated with existing Microsoft Active Directory or LDAP systems to have fine-grained role based access control over cloud resources[8].

Eucalyptus supports storage area network devices to take advantage of storage arrays to improve performance and reliability. Eucalyptus Machine Images can be backed by EBS-like persistent storage volumes, improving the performance of image launch time and enabling fully persistent virtual machine instances. Eucalyptus also supports direct-attached storage.

VI CONCLUSION

It is used to build private, public and hybrid clouds. It can also produce your own datacenter into a private cloud and allow you to extend the functionality to many other organizations. Eucalyptus provides APIs to be used with the web services to cope up with the demand of resources used in the private clouds.

REFERENCES

[1]. Buyya, R., C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic (2009). Cloud computing and emerging {IT} platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599 – 616. ISSN 0167-739X. URL http://www.sciencedirect.com/science/article/pii/

S0167739X08001957.

[2]. Dalcin, L. (2012). MPI for Python, Release 1.3. URL http://mpi4py.scipy.org//.

[3]. Eucalyptus Systems, I. (a). Eucalyptus 3.1.2 Installation Guide. URL https:// www.eucalyptus.com/.

[4]. Eucalyptus Systems, I. (b). Eucalyptus 3.1.2 User Guide. URL https://www.eucalyptus.com/.

[5]. Gibson, J., R. Rondeau, D. Eveleigh, and Q. Tan, Benefits and challenges of three cloud computing service models. In Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on. 2012.

[6]. Gong, C., J. Liu, Q. Zhang, H. Chen, and Z. Gong, The characteristics of cloud computing. In Parallel Processing Workshops (ICPPW), 2010 39th International Conference on. 2010. ISSN 1530-2016.

[7]. He, H., Applications deployment on the saas platform. In Pervasive Computing and Applications (ICPCA), 2010 5th International Conference on. 2010.

[8]. He, Q., S. Zhou, B. Kobler, D. Duffy, and T. McGlynn, Case study for running hpc applications in public clouds. In Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing, HPDC '10. ACM, New York, NY,USA, 2010. ISBN 978-1-60558-942-8. URL http://doi.acm.org/10.1145/1851476.1851535.

 ISBN: 978-81-931039-3-7

TOP THREATS IN CLOUD COMPUTING

Pooja Sharma[1], Rajkumar Singh Rathore[2]

[1]PG Scholar, Masters of Technology ,
Galgotias College of Engineering and Technology, Greater Noida (India)
[2] Assistant Professor , Department of Computer Science & Engineering
Galgotias College of Engineering & Technology, Greater Noida (India)

ABSTRACT

The purpose of this document, "Top Threats to Cloud Computing", is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies. Many believe that Cloud is reshaping the entire IT industry as a revolution. Today rapid development in web technologies such as blogging, social networking, online media sharing etc. has moving bulk of data onto internet servers. Because of this there arises a need for companies to adopt utility or cloud computing. In this paper, we aim to point out the challenges and security issues in cloud computing as today, security and privacy concerns may represent the biggest hazards to moving services to external clouds. This paper outlines the brief description of cloud delivery and deployment models, cloud security advantages and disadvantages and then detailed discussion of issues and security threats relating to its implementation, datalocation and storage, management, virtualization etc in the Cloud. The aim is to provide some useful security related information for organizations having their data on clouds or for those preparing to migrate to the cloud to take advantage of this latest computing paradigm.

Keywords: Cloud computing; Security; Public cloud; Private cloud; Hybrid cloud; policies; Security challenges; Cloud security model

I. INTRODUCTİON

Cloud computing has recently emerged as a buzz word in the distributed computing community. Many believe that Cloud is going to reshape the IT industry as a revolution. It is a business model that has inherited the benefit of other technologies such as distributed, pervasive, ubiquitous, utility computing and virtualization [4]. So, what is cloud computing? How these computing services providing ease for organizations to manage and save its data to the cloud? What are the issues and challenges for both cloud providers and its consumers?Here we start with first what is cloud computing:

Definition: Cloud computing is a model for enabling 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[1].

This definition includes everything about a cloud regarding to its architectures, security and deployment strategies. In particular, five essential elements of cloud computing areclearly mentioned:

- *On-demand self-service*: A consumer with an instantaneous need at a particular timeslot can avail computing resources (such as CPU time, network storage, software use, and so forth) in an automatic (i.e. convenient, self-serve) fashion.
- *Broad network access*: These computing resources are delivered over the network (e.g. Internet) and used by various client applications with heterogeneous platforms (such as mobile phones, laptops, and PDAs) situated at a consumer's site.
- *Resource pooling*: A cloud service provider's computing resources are 'pooled' together in an effort to serve multiple consumers using either the *multi-tenancy* or the *virtualization* model, "with different physical and virtual resourcesdynamically assigned and reassigned according to consumerdemand".
- *Rapid elasticity*: For consumers, computing resources become immediate rather than persistent: there are no up-front commitment and contract as they can use them to scale up whenever they want, and release them once they finish to scale down.
- *Measured Service*: Although computing resources are pooled and shared by multiple consumers (i.e. multi-tenancy), the cloud infrastructure is able to use appropriate mechanisms to measure the usage of these resources for each individual consumer through its metering capabilities.
- Enterprises are now beginning to develop and deploy management software to deal with scaled Cloud environments [2]. They all are also developing their standards and policies for dealing with types of Clouds.
- The rest of this paper is organized as follows. Section 2 outlines the Cloud delivery and deployment approaches. Then, Sections 3rd and 4th discuss, in brief, the advantages and disadvantages of Cloud security and the inherent issues and challenges. The last section consists of the conclusion.

II. CLOUD COMPUTING

2.1 Delivery Models

As shown in *Fig. 1*, the Cloud model consists of, three types of services: Software Services, Platform Services and Infrastructure services. These services are related to three delivery models of Cloud, defined as follows:

- *Software as a service (SaaS)*: allows the users to utilize various applications from the cloud rather than using applications on their own computer. Normally it refers to prebuilt pieces of software or complete applications like an email system, database processing, human resource management, etcwhich are provided as services.
- *Platform as a service (PaaS)*: operates at a lower level than the SaaS. It is responsible for the management of the storage space, bandwidth allocation and computing resources available for the applications. This model refers to application development toolkits and deployment tools e.g. application servers, portal servers and middleware and consumers use these to build and deploy their own applications.
- *Infrastructure as a service (IaaS)*: This refers to infrastructure-centric IT resources such as visualized servers, storage, network devices, operating systems, etc as well as hardware services to enable Cloud platforms and software to operate. It dynamically scales bandwidth allocation and server resources for the cloud. This service allows the cloud to operate during high traffic/demanding situations as resources are dynamically increased as they are needed [2].

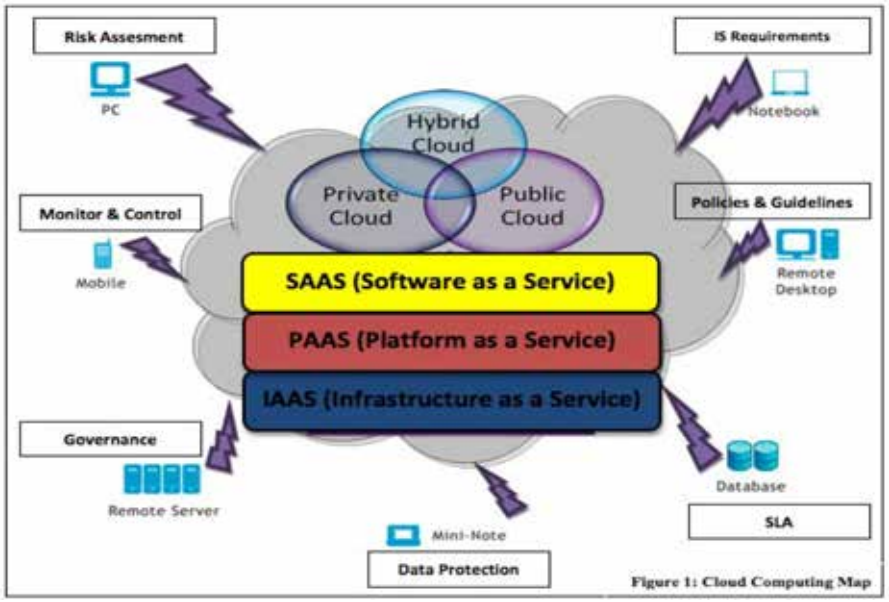


Figure1. Cloud Computing Map [5]

2.2 Deployment Approaches

There are three main types of cloud deployment models - public, private and hybrid clouds[10].

- *Public Clouds* – are the most common type of cloud. This is where multiple customers can access web applications and services over the internet. It's typically based on a pay-per-use model. Each individual customer has their own resources which are dynamically provisioned by a third party vendor. This third party vendor hosts the cloud for multiple customers from multiple data centers (see Figure 2), manages all the security and provides the hardware and infrastructure for the cloud to operate. The customer has no control or insight into how the cloud is managed or what infrastructure is available. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network[11]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attack [5].

- *Private Clouds* – emulate the concept of cloud computing on a private network. They allow users to have the benefits of cloud computing without some of the pitfalls. A private cloud is setup within an organisation's internal enterprise datacenter. Private clouds grant complete control over how data is managed and what security measures are in place. This can lead to users having more confidence and control. In this Cloud users can easily share and use the scalable resources and virtual applications (that are pooled together) provided by the cloud vendor. Utilization on the private cloud can be much more secure because of its specified internal exposure. The major issue with this deployment model is that the users have large expenditures as they have to buy the infrastructure to run the cloud and also have to manage the cloud themselves.

- *Hybrid Clouds* – Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models [11]. It provides virtual IT solutions through a mix of both public and private clouds (provisioned as a same unit) within the same network. Hybrid Clouds provide more secure control of the data and applications. For example, an organisation could hold sensitive information on their private cloud and use the public cloud for handling large traffic and demanding situations.

To summarise, in the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand [5]. Security considerations are the measure issue in deciding which type of cloud to deploy from an enterprise architectural point of view. Hence, there is a need of taking into account the information security differences of each model discussed above.

III CLOUD THREATS

There has been much debate about what is "in scope" for this research. We expect this debate to continue and for future versions of "Top Threats to Cloud Computing" to reflect the consensus emerging from those debates. While many issues, such as provider financial stability, create significant risks to customers, we have tried to focus on issues we feel are either unique to or greatly amplified by the key characteristics of Cloud Computing and its shared, on-demand nature. We identify the following threats
in our initial document:

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service & Traffic Hijacking
7. Unknown Risk Profile

1) Abuse and Nefarious Use of Cloud Computing

Description

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Examples

IaaS offerings have hosted the Zeus botnet, InfoStealer trojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam

continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

Remediation

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

2) Insecure Interfaces and APIs

Description

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to thirdparties in order to enable their agency.

Examples

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities,
unknown service or API dependencies.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Impact

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

3) Malicious Insiders

Description

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined

with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Examples

No public examples are available at this time.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Impact

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

4) Shared Technology Issues

Description

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (*e.g.*, CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Examples

- Joanna Rutkowska's Red and Blue Pill exploits
- Kortchinksy's CloudBurst presentations.

Remediation

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.

- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Impact

Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

5) Data Loss or Leakage

Description

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Examples

Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; persistence and remanence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.

Remediation

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Impact

Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

6) Account or Service Hijacking

Description

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect

your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Examples

No public examples are available at this time.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Impact

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

7) Unknown Risk Profile

Description

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Examples

- IRS asked Amazon EC2 to perform a C&A; Amazon refused.
  http://news.qualys.com/newsblog/forrester cloud-computingqa. html
- Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected, but Heartland was "willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen."
  http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html

Remediation

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information

Impact

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

IV CONCLUSION

In this paper, we explored the security issues and challenges at various domains of cloud computing. We reviewed the present ongoing security issues to make the customers aware of the problem that will arise in cloud computing paradigm. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. However, one must be very careful to understand the security risks and challenges posed during utilization of these cloud computing technologies. Hence our concern is to provide a collective review of all these present issues in a single paper to provide ease to the cloud customers.

REFERENCES

[1] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud computing : issues and challenges," IEEE, 2010 [24th IEEE International Conference on Advanced Information Networking and Applications].

[2] ZaighamMahmood, "Data location and security issues in cloud computing," IEEE, 2011 [International conference on Emerging Intelligent Data and Web Technologies].

[3] Sara Hamounda, "Security and privacy in cloud computing," IEEE, 2012 [International Conference on Cloud Computing, Technologies, Applications & Management].

[4] Mervat Bamiah, Sarfraz Bohri, Suriayati Chuprat, Muhammad Nawaz Brohi, "Cloud implementation security challenges," IEEE, 2012 [International Conference on Cloud ComputingTechnologies, Applications& Management].

[5] Ramgovind S, Eloff MM and Smith E, "The management of security in cloud computing," IEEE, 2010.

[6] GurudattKulkarni, JayantGhambhir, TejswiniPatil, Amruta Dongare, "A security aspects in cloud computing," IEEE, 2012.

[7] AkhilBehl, KanikaBehl, "An analysis of cloud computing Security Issues," IEEE, 2012.

[8] Hsin-Yi Tsai, Melanie Siebenhaar, Andre Miede, Yu-Lu Huang, Ralf Steinmetz, "Threat as a service? Virtualization's impact on cloud security," IEEE, January/February 2012.

[9] Xiangyang Lou, Lin Yang, Linru Ma, Shanming Chu, Hao Dai, "Virtualization security risks and solutions of cloud computing via divide-conquer strategy," IEEE, 2011 [Third International conference on Multimedia Information Networking and Security].

[10] Sean Carlin, Kevin Curran, "Cloud Computing Security," International Journal of Ambient Computing and Intelligence, pp. 14-19, January-March 2011.

[11] Google. (2014). Cloud computing – Wikipedia. [online]. Available:http://en.wikipedia.org/wiki/Cloud_computing.

CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES

Disha Bhatnagar[1], Rajkumar Singh Rathore[2]

[1]PG Scholar, Masters of Technology ,
Galgotias College of Engineering and Technology, Greater Noida (India)
[2] Assistant Professor, Department of Computer Science & Engineering
Galgotias College of Engineering & Technology, Greater Noida (India)

ABSTRACT

Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. Cloud computing is a fast growing information technology, has aroused the concern of the whole world. This is a favorable situation to study and application of cloud computing related technologies. However, most existing Cloud Computing platforms have not formally adopted the service-oriented architecture (SOA) that would make them more flexible, extensible, and reusable. The security aspects in a cloud based computing environment remains at the core of interest. We have categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained.

Keywords : ***Cloud Architecture , Security Concerns, Security Measures and Counter Attacks in Cloud Computing ,CCOA, Iaas, OSI Model, Paas, SaaS , SOA,***

I INTRODUCTION

Cloud computing is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices. 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 Recent

developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

1. The transmission of personal sensitive data to the cloud server,
2. The transmission of data from the cloud server to clients' computers and
3. The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

Cloud computing has several distinct characteristics that distinguish it from a traditionally-hosted computing environment:

- Users often have on-demand access to scalable information technology capabilities and services that are provided through internet-based technologies.
- These resources run on an external or third-party service provider's system. This is in contrast to traditional systems, which run on locally-hosted servers. Unlike traditional systems which are under the user's personal control or institutional control, cloud computing services are fully managed by the provider.
- Typically, many unaffiliated and unconnected users share the service provider's infrastructure.
- Using cloud services reduces the need to carry data on removable media because of network access anywhere, anytime.

Cloud services, sometimes called "software as a service" (SaaS) ,"infrastructure as a service" (IaaS), or "platform as a service" (PaaS), facilitate rapid deployment of applications and infrastructure without the cost and complexity of purchasing, managing, and maintaining the underlying hardware and software.

II. SERVICES IN CLOUD

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid International Journal of Network Security & Its Applications and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion .

The services provided by cloud providers can be divided into following three main layered categories. Each layer consumes services provided by the layer below it.

1. Software as a service (SAAS)

SaaS clients rent usage of applications running within the Cloud‟s provider infrastructure, for example SalesForce . The applications are typically offered to the clients via the Internet and are managed completely by the Cloud provider. That means that the administration of these services such as updating and patching are in the provider's responsibility. One big benefit of SaaS is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients.

2. Platform as a service (PAAS)

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

3. Infrastructure as a service (IAAS)

IaaS delivers hardware resources such as CPU, disk space or network components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. The client has full control of the virtualized platform and is not responsible for managing the underlying infrastructure.

4. Storage as a service

Storage as a service (STaaS) is a business model in which a large service provider rents space in their storage infrastructure on a subscription basis. The economy of scale in the service provider's infrastructure allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered. Storage as a Service is often used to solve offsite backup challenges**.** Critics of storage as a service point to the large amount of network bandwidth required to conduct their storage utilizing an internet-based service.

5. Security as a service

Security as a service (SCaaS) is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

6. Data as a service

Data as a service, or DaaS, is a cousin of software as a service. Like all members of the "as a Service" (aaS) family, DaaS is based on the concept that the product, data in this case, can be provided on demand to the user regardless of geographic or organizational separation of provider and consumer. Additionally, the emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant.

III. CLOUD COMPUTING SECURITY

When talking about a cloud computing system , it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. opensource vs. proprietary) might pose security threat and concerns which, of course, is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing Any security tools or other kinds of software. used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment. As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach . The approach by which cloud computing is done has made it prone to both information security and network security issues .

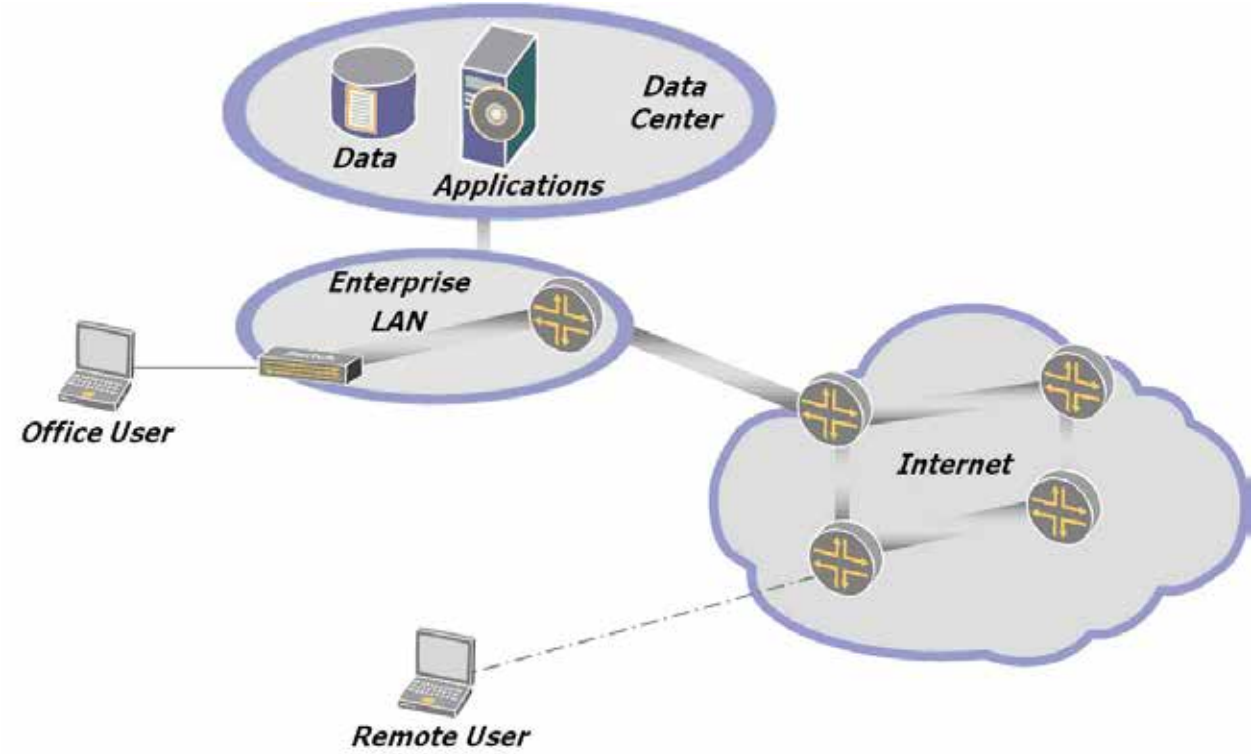


Fig 1: Cloud Computing Model

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines. If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy**.**

3.1 Security Concerns of Cloud Computing Architecture

Principle 1: Overall Security Concerns

[1] Gracefully lose control while maintaining accountability even if operational responsibility falls upon 3rd parties.

[2] Provider, user security duties differ greatly between cloud models 22 Governance.

[3] Identify, implement process, controls to maintain effective governance, risk mgt, compliance

[4] Provider security governance should be assessed for sufficiency, maturity, consistency with user ITSEC process 3 rd Party Governance

[5] Request clear docs on how facility & services are assessed

[6] Require definition of what provider considers critical services, information.

[7] Perform full contract, terms of use due diligence to determine roles, accountability 24 Legal, e-Discovery

[8] Functional: which functions & services in the Cloud have legal implications for both parties.

[9] Jurisdictional: which governments administer laws and registrations impacting services, stakeholders, data assets .

[10] Both parties must understand each other's roles – Litigation hold, Discovery searches – Expert testimony • Provider must save primary and secondary (logs) data.

PRINCIPLE 2: Bigger Security Concerns For Cloud Computing

There are two basic approaches for enabling virtualization in the Cloud Computing environment.

a. Hardware virtualization that is to manage hardware equipment in plug-and-play mode.

b. Software virtualization, i.e., to use software image management or software code virtualization technology to enable software sharing.

• **Management interface vulnerability**. Consumer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than traditional hosting providers and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

• **Data protection**. Cloud computing poses several data protection risks for cloud consumers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud consumer (in the role of data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated cloud services.

• **Malicious behavior of insiders**. Damage caused by the malicious actions of insiders working within an organization can be substantial, given the access and authorizations they may have. This is compounded in the cloud computing environment since such activity might occur within either or both the consumer organization and the provider organization.

• **Business failure of the provider**. Such failures could render data and applications essential to the consumer's business unavailable.

• **Service unavailability**. This could be caused by a host of factors, from equipment or software failures in the provider's data center, through failures of the communications between the consumer systems and the provider services.

• **Insecure or incomplete data deletion**. Requests to delete cloud resources, for example,when a consumer terminates service with a provider, may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a consumer perspective), either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other clients. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the consumer than is the case with dedicated hardware.

PRINCIPLE 3: MANAGING SECURITY IN CLOUD

Since cloud computing typically involves two organizations - the service consumer and the service provider, security responsibilities of each party must be made clear. This is typically done by means of a service level agreement (SLA) which applies to the services provided, and the terms of the contract between the consumer and the provider. The SLA should specify security responsibilities and should include aspects such as the reporting of security breaches. SLAs for cloud computing are discussed in more detail in the CSCC document "Practical Guide to Cloud Service Level Agreements. One feature of an SLA relating to security is that any requirements that are placed on the cloud provider by the SLA must also pass on to any peer cloud service providers that the provider may use in order to supply any part of their service(s). It should be explicitly documented in the cloud SLA that providers must notify consumers about the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur

IV. EXAMINING SECURITY REQUIREMENTS OF EXIT PROCESS

The exit process or termination of the use of a cloud service by a consumer requires careful consideration from a security perspective. From a security perspective, it is important that once the consumer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the consumer's data should remain with the provider. The provider must ensure that any copies of the data are wiped clean from the provider's environment, wherever they may have been stored (i.e. including backup locations as well as online data stores). Note that other data held by the provider may need "cleansing" of information relating to the consumer (e.g. logs and audit trails), although some jurisdictions may require retention of records of this type for specified periods by law. Clearly, there is the opposite problem during the exit process itself - the consumer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the consumer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.

.

V. CONCLUSION

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect could infrastructures and software. The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impact. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. To welcome the coming cloud computing era, solving the existing issues becomes utmost importunity.

REFERENCES

[1] Web-Resource http://en.wikipedia.org/wiki/Cloud_computing

[2] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

[3] Cloud Computing and Grid Computing 360-Degree Compared by Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. (IEEE Conference, **Date of Conference:** 12-16 Nov. 2008)

[4] Cloud Computing: a Perspective Study Lizhe WANG, Gregor VON LASZEWSKI

[5] http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm

[6] Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513- 521. http://dx.doi.org/10.1016/j.clsr.2012.07.002

[7] Liang-Jie Zhang and Qun Zhou, CCOA: Cloud Computing Open Architecture 2009 IEEE International Conference on Web Services, 2009.

[8] http://en.wikipedia.org/wiki/Virtualization

[9] http://www.dummies.com/how-to/content/how-to-use-virtualization-with-cloud-computing.html

International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science
DAVIM, Faridabad, 25th April, 2015 ISBN: 978-81-931039-3-7

CLOUD COMPUTING: ARCHITECTURE AND CONCEPT OF VIRTUALIZATION

Neha Roy[1], Rishabh Jain[2]

[1]PG Scholar, Masters of Technology ,
Galgotias College of Engineering and Technology, Greater Noida (India)
[2] Assistant Professor, Department of Computer Science & Engineering
Galgotias College of Engineering & Technology, Greater Noida (India)

ABSTRACT

Technology innovation and its adoption are two critical successful factors for any business/organization. Cloud computing is a recent technology paradigm that enables organizations or individuals to share various services in a seamless and cost-effective manner. This paper describes cloud computing, a computing platform for the next generation of the Internet. The paper defines clouds, types of cloud Provides, Comparison of Cloud Computing with Grid Computing, applications and concerns of Cloud Computing , Concept of Virtualization in Cloud Computing. Cloud computing is beginning from the development of parallel computing, distributed computing, shared computing and grid computing. For the sharing resources that contains software, applications, infrastructures and business processes, cloud computing is the main key. Cloud computing has brought new tremendous changes and good opportunities to information technology industry. Cloud computing is a fast growing information technology, has aroused the concern of the whole world. This is a favorable situation to study and application of cloud computing related technologies. However, most existing Cloud Computing platforms have not formally adopted the service-oriented architecture (SOA) that would make them more flexible, extensible, and reusable. By bridging the power of SOA and virtualization in the context of Cloud Computing ecosystem, this paper presents seven architectural principles

Keywords : ***Cloud Architecture , Computing Applications and Concerns, Cloud Computing vs. Grid Computing ,CCOA, Iaas, OSI Model, Paas, SaaS , SOA, Virtualization***

1. INTRODUCTION

Cloud computing [1] is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices. Cloud computing [2] 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. Cloud Computing provides environments to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications. The operation models may include pay-as-go utility models, free infrastructure services with value added platform services, fee-based infrastructure services with value-added application services, or free services for vendors but sharing of revenues generated from consumers. "Cloud Computing is the delivery of application softwares, infrastructure and platform as a service over the Internet accessible from the web browser and desktop with the end user not having any knowledge of the service providing system, platform, as well as of where the software and data are residing on the servers on a pay-per-use basis."

Definition :

A cloud is a pool of virtualized computer resources. A cloud can:

1. Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications.
2. Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines.
3. Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures
4. Monitor resource use in real time to enable rebalancing of allocations when needed.

Cloud Computing vs Grid Computing:

Cloud computing environments support grid computing by quickly providing physical and virtual servers on which the grid applications can run. Cloud computing should not be confused with grid computing [3]. Grid computing involves dividing a large task into many smaller tasks that run in parallel on separate servers. Grids require many computers, typically in the thousands, and commonly use servers, desktops, and laptops. Clouds also support nongrid environments, such as a three-tier Web architecture running standard or Web 2.0 applications. A cloud is more than a collection of computer resources because a Cloud provides a mechanism to manage those resources. Management includes provisioning, change requests, reimaging, workload rebalancing, deprovisioning, and monitoring.

II. CLOUD SERVICES

The services provided by cloud providers can be divided into following three main layered categories. Each layer consumes services provided by the layer below it.

1. Software as a service (SAAS) :

SaaS clients rent usage of applications running within the Cloud‟s provider infrastructure, for example SalesForce. The applications are typically offered to the clients via the Internet and are managed completely by the Cloud provider. That means that the administration of these services such as updating and patching are in the provider‟s responsibility. One big benefit of SaaS [4] is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients.

2. Platform as a service (PAAS) ;

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

3. Infrastructure as a service (IAAS) ;

IaaS delivers hardware resources such as CPU, disk space or network components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. The client has full control of the virtualized platform and is not responsible for managing the underlying infrastructure.

4. Storage as a service ;

Storage as a service (STaaS) is a business model in which a large service provider rents space in their storage infrastructure on a subscription basis. The economy of scale in the service provider's infrastructure allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered. Storage as a Service is often used to solve offsite backup challenges**.** Critics of storage as a service point to the large amount of network bandwidth required to conduct their storage utilizing an internet-based service.

5. Security as a service ;

Security as a service (SECaaS) is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

6. Data as a service ;

Data as a service, or DaaS, is a cousin of software as a service. Like all members of the "as a Service" (aaS) family, DaaS is based on the concept that the product, data in this case, can be provided on demand to the user regardless of

geographic or organizational separation of provider and consumer. Additionally, the emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant.

III. CLOUD COMPUTING ARCHITECTURE

When talking about a cloud computing system [5], it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

Fig 1: Cloud Computing Architecture

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines. If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of

storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy**.**

3.1 Seven Principles of Cloud Computing Architecture

In this Cloud Computing Open Architecture, we propose an integrated co-innovation and co-production framework to get cloud vendors, cloud partners, and cloud clients to work together based on seven principles. The presented Cloud Computing Open Architecture covers cloud ecosystem enablement, cloud infrastructure and its management, service-orientation, cloud core on provisioning and subscription, compostable cloud offerings, cloud information architecture and management, and cloud quality analytics. This is a logical and modularized separation, which helps isolate concerns of details of each module during the design process. Since the connections between the identified key architectural principles for Cloud Computing are quite complex, the information exchanges are going through the Cloud Information Architecture and Cloud Ecosystem Management. In the rest of the section, we will introduce the details of each principle

PRINCIPLE 1: INTEGRATED ECOSYSTEM MANAGEMENT FOR CLOUD

Architecture must support the management of the ecosystem of Cloud Computing. This ecosystem includes all involved services and solutions vendors, partners, and end users to provide or consumer shared resources in the Cloud Computing environment. The Cloud Computing ecosystem management layer (1A) provides an integrated on-boarding process and common utilities to hosting environment are used to support the frontend’s operations. support the seamless collaboration and message exchanges among cloud vendors, partners, and clients. For example, the onboard progress covers the registration of business entities and users. The business entities include cloud vendors, cloud partners, and enterprise cloud clients. The user entities are end users within a certain business entity (e.g. an employee of a company, or a member of a registered community like a social network), or consumer users in the open Internet space [6] [7].

PRINCIPLE 2: VIRTUALIZATION FOR CLOUD INFRASTRUCTURE

There are two basic approaches for enabling virtualization in the Cloud Computing environment.

a. Hardware virtualization that is to manage hardware equipment in plug-and-play mode.

b. Software virtualization, i.e., to use software image management or software code virtualization technology to enable software sharing.

It is noted that this virtualization principle in the Cloud Computing Open Architecture is an extension of the operational system layer in the SOA Solution Stack (also known as SOA Reference Architecture) in the context of Cloud Computing enablement [7].

PRINCIPLE 3: SERVICE-ORIENTATION FOR COMMON

Service-orientation is another driving force to enable Cloud Computing to further realize the business value from asset reusability, composite applications, and mashup services. There are two major types of common reusable services: Cloud Horizontal and Vertical Business Services. The Cloud Horizontal Business Services consist of various platform services that hide the complexities of middleware, database, and tools. The Cloud Vertical Business Services include all domain specific or industry-specific utility services [7].

PRINCIPLE 4: EXTENSIBLE PROVISIONING AND SUBSCRIPTION FOR CLOUD

Extensible service provisioning is the unique feature of a Cloud Computing system. Without extensibility, the provisioning part of the Cloud Computing architecture can only support a certain type of resource sharing. This implies that the service provisioning architecture for free use users and paying users are the same. Both types of users can be service providers or consumers from time to time. From service consumers' perspective, they are interested in how to easily access services based on their own business logics and goals [7].

PRINCIPLE 5: CONFIGURABLE ENABLEMENT FOR CLOUD OFFERINGS

Cloud offerings are the final products or services that are provisioned by the Cloud Computing platform. Since all cloud offerings should address certain business goals, cloud offerings are also known as cloud business solutions. Example of cloud offerings is storage cloud and infrastructure cloud. Most cloud offerings are delivered or accessed through Web browsers [7].

PRINCIPLE 6: UNIFIED INFORMATION REPRESENTATION AND EXCHANGE FRAMEWORK

Information representation and message exchange of Cloud Computing resources are very important to enable the collaborative and effective features of Cloud Computing. In CCOA, Cloud Computing resources include all business entities (e.g. cloud clients, partners, and vendors) and the supporting resources such as virtualization related modules, service-orientation related modules, cloud core, and cloud offerings. Just like blood in human bodies, the cloud information architecture uses its information "blood" to form "blood stream" to get all various modules to communicate with each other in an effective way in CCOA [7].

PRINCIPLE 7: CLOUD QUALITY AND GOVERNANCE

The last and most important module in CCOA is the Cloud Quality and Governance. This Section is responsible for the identification and definition of quality indicators for Cloud Computing environment and a set of normative guidance to govern the design, deployment, operation, and management of the cloud offerings. From quality indicators' perspective, Quality of Services (QoS) parameters can be directly used to define cloud entities' reliability, response time, security, and integrity. The integrity can be checked through traceability enablement and compliance validation. Security is a very important aspect of the cloud quality [7].

IV. VIRTUALIZATION IN CLOUD COMPUTING

Any discussion of cloud computing typically begins with virtualization [8]. *Virtualization* is using computer resources to imitate other computer resources or whole computers. It separates resources and services from the underlying physical delivery environment.

Characteristics

Virtualization has three characteristics that make it ideal for cloud computing:

1) Partitioning: In virtualization, many applications and operating systems (OSes) are supported in a single physical system by *partitioning* (separating) the available resources.

2) Isolation: Each virtual machine is isolated from its host physical system and other virtualized machines. Because of this isolation, if one virtual-instance crashes, it doesn't affect the other virtual machines. In addition, data isn't shared between one virtual container and another.

3) Encapsulation: A virtual machine can be represented (and even stored) as a single file, so you can identify it easily based on the service it provides. In essence, the encapsulated process could be a business service. This encapsulated virtual machine can be presented to an application as a complete entity. Therefore, encapsulation can protect each application so that it doesn't interfere with another application.

Applications of virtualization

Virtualization can be applied [9] broadly to just about everything that you could imagine:

1) Memory
2) Networks
3) Storage
4) Hardware
5) Operating systems
6) Applications

What makes virtualization so important for the cloud is that it decouples the software from the hardware. *Decoupling* means that software is put in a separate container so that it's isolated from operating systems.

Forms of virtualization

To understand how virtualization helps with cloud computing, you must understand its many forms. In essence, in all cases, a resource actually emulates or imitates another resource. Here are some examples:

1) Virtual memory: Disks have a lot more space than computer memory. Therefore, with virtual memory, the computer frees valuable memory space by placing information it doesn't use often into disk space. PCs have *virtual memory*, which is a disk area that's used like memory. Although disks are very slow in comparison with memory, the user may never notice the difference, especially if the system does a good job of managing virtual memory. The substitution works surprisingly well.

2) Software: Companies have built software that can emulate a whole computer. That way, one computer can perform as though it were actually 20 computers. The application consolidation results can be quite significant. For example, you might be able to move from a data center with thousands of servers to one that supports as few as a couple of hundred. This reduction results in less money spent not only on computers, but also on power, air conditioning, maintenance, and floor space.

V. CONCLUSION

In today's global competitive market, companies must innovate and get the most from its resources to succeed. This requires enabling its employees, business partners, and users with the platforms and collaboration tools that promote innovation. Cloud computing infrastructures are next generation platforms that can provide tremendous value to companies of any size. Cloud Computing provides Software, Platform, Infrastructure, Storage, Security, Data, Test Environment etc. as a service. I also discussed the Concept of Virtualization in Cloud Computing as any discussion of cloud computing typically begins with the virtualization. Virtualization is using computer resources to imitate other computer resources or whole computers. I discussed the characteristics, applications and various forms of Virtualization. In this paper, I have proposed the Cloud Computing Open Architecture (CCOA) based on seven architectural principles by integrating the power of service-oriented architecture (SOA) and virtualization technology of hardware and software. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. To welcome the coming cloud computing era, solving the existing issues becomes utmost importunity!

REFERENCES

[1] Web-Resource http://en.wikipedia.org/wiki/Cloud_computing

[2] Galen Gruman and Eric Knorr. What cloud computing really means. InfoWorld, April 2008. Electronic Magazine, available at http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality 1.html.

[3] Cloud Computing and Grid Computing 360-Degree Compared by Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. (IEEE Conference, **Date of Conference:** 12-16 Nov. 2008)

[4] Cloud Computing: a Perspective Study Lizhe WANG, Gregor VON LASZEWSKI

[5] http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm

[6] John Y. Sayah, Liang-Jie Zhang, On-demand business collaboration enablement with web services, Decision Support System, 40 (2005), pp.107-127.

[7] Liang-Jie Zhang and Qun Zhou, CCOA: Cloud Computing Open Architecture 2009 IEEE International Conference on Web Services, 2009.

[8] http://en.wikipedia.org/wiki/Virtualization

[9] http://www.dummies.com/how-to/content/how-to-use-virtualization-with-cloud-computing.html

THE INFLUENCE OF SOCIAL MEDIA ON INDIAN TEENAGERS

Dr. Anamika Bhargava[1] , Minaxi Rani[2]

[1]*Associate Professor, DAV Institute of Management, NH-3, NIT, Faridabad-121002, Haryana, (India)*

[2]*Extn. Lecturer, Commerce Department, N.M Govt. P.G. College , Hansi-125022 , Haryana, (India)*

ABSTRACT

In the last few years, Social Network Media have spread widely all over the world and are used by various users for several reasons and purpose. The influence of social websites can be good on students but if we have a closer look on the real impact of social media[1]. Today it is ruining the carrier and future of students. Today 2.5 billion people across the world have their profiles in social networking Media. Everything looks nice when you create a profile on social Media websites, but how you feel when hackers start blackmailing using your personal information. The social media websites are www.linkedin.com, www.facebook.com, www.twitter.com and www.orkut.com etc. are continuously distracting students from their studies. The main focus of students should be education but unfortunately today's students are emphasizing on such sites which can be a complete wastage of time. It has become an addiction for college students, teenagers and adults also. This paper presents impact of social media on Indian education, students and impact on teenager's life, further it describes how social media networking websites are auditory and dangerous for Indian youth and teenagers.

Keywords: Social Media, Education, Students, Influence Of Social Networking Sites.

I INTRODUCTION

Internet is now necessary part of life from shopping to electronic mails and education. It is a very large community, which is using internet for education but unluckily we have also a very large number of people including majority of youth and teenagerusing Internet only for using social media. Internet is very big evolution of technology but when we talk about the social media. The social media is "the relationships that exist between network of people". Thanks to the invention of social media, young men and women now exchange ideas, feelings, personal information, pictures and videos at a truly astonishingrate. 164.81 million of wired Indian teens and Students now use social media websites (According to The Telecom Regulatory Authority of India (TRAI))[1]. It is extremely dangerous for youth and become extremely common and widespread in the last few years. However, every day, many students are spending countless hours immersed in social media websites. The basic phenomena of social media sites is very easy to understand, it is a web based facility which allows individual user to build a profile identity and generate subjective associations and connections among himself and list of other friends and communicate with them at a central location. These websites are powered by many international companies because these websites are centrally

visited by millions of people thus companies can get benefit of advertisements, this is how social networks are get paid; user can register himself free of cost in social networking sites like www.facebook.com, www.orkut.com, www.linkedin.com and www.twitter.com etc[1]. Peoples are get connected to one another after registration and then post information, fake news, fake videos and other things including images etc. Through social networking, people can use networks of online friends and group memberships to keep in touch with current friends, reconnect with old friends or create real life friendships through similar interests or groups. Besides establishing important social relationships, social networking members can share their interests with other like minded members by joining groups and forums. Some networking can also help members find a job or establish business contacts. Most social networking websites also offer additional features. In addition to blogs and forums, members can express themselves by designing their profile page to reflect their personality. The most popular extra features include music and video sections. The video section can include everything from member generated videos from hundreds of subjects to TV clips and movie trailers (Youtube).

II HISTORY OF SOCIAL NETWORKING MEDIA

In mid of 1990's social media sites are born with Web 2.0 technology included www.Classmates.com in 1995 focusing on ties with former school mates, and www.SixDegrees.com in 1997 focusing on indirect ties. User profiles can be created, messages sent to a friends list and other members found out from their profiles[2]. These websites are simply were not profitable and eventually shut down due to fewer features. In 2003 a new face of social network website www.linkedin.com and www.myspace.com was reportedly getting more page views than Google, with Facebook, a competitor, rapidly growingin size. In 2005, www.Facebook.com began allowing externally-developed add-on applications, and some applications enabled the graphing of a user's own social network - thus linking social networks and social networking. www.orkut was quietly launched on January 22, 2004 by Google, the search engine company which is now quite popular in India, U.S.A and Brazil[3].

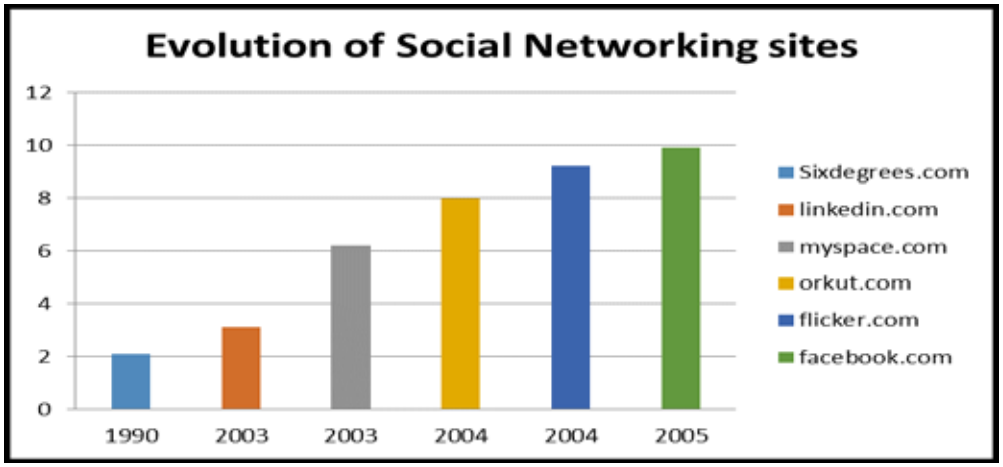


Figure 1.1(A) Shows the Evolution of Social Networks from 1990 To 2005

III RESEARCH APPROACH

When we talking about the law and jurisdiction about social media networking unfortunately, we don't have any law for Social networks in India, as it is international law that user must be minimum 18 years older more to register

yourself in any social media website. We don't have any authority to check the user details if user is below 18 year age or above 18 year age. This research employs the method of Qualitative research through research analysis to gather an in-depth understanding of the behavioral changes caused by the social media websites.

After a survey it has been analyzed that one of very large number of underage users, using social media websites, one user can have one Identity or profile at the sametime but according to survey one user is facilitating him by fake identities on same time as shown in figure 1.2.

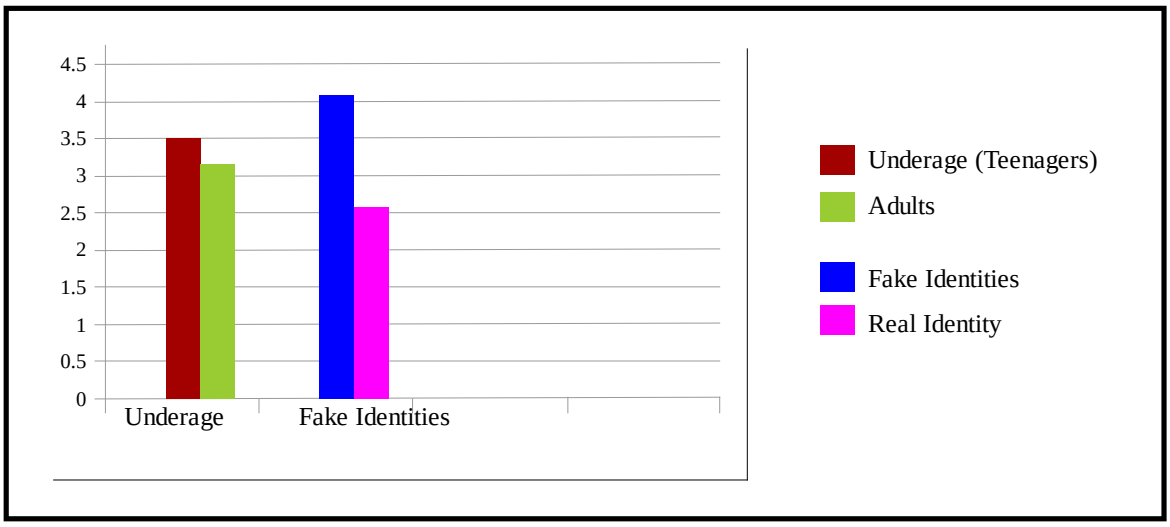


Fig. 1.2 Graph Representations Of Underage User And Fake Identities

In this above Figure 1.2 shows the average of fake identities and underage users. According to the research analysis survey a very large number of fake identities exist in social media networks, these fake identities perform many kind of violations on social media Networks in which they register themselves as a fake identity on name of someone else and upload of unseemly material (Porn or adult videos and images) with fake identities this is a common act of violation[2].

IV RESEARCH METHODS

The research has made use of research analysis survey. This Survey was conducted among randomly selected social networking sites users in India with a age group of 16 to 22 yrs old students or teenagers. The age group youth 16 to 22 years was chosen since they are the heavy user of social media sites and also early adopters of advanced Application of Information technology. Another reason for choosing this age group is that:

Youth (students or teenagers) of the age group 16 to 22 years:-

- Ø View world idealistically
- Ø they involved with world's outside youth
- Ø Relationship equalize in that
- Ø See all adults as equal

The surveys were done using web 2.0 service, where the questions are disseminate through survey's websites, e-mail and some datas were collected through personal interview or through telephonic interview also. The data were

collected through direct conversation and had face-to-face conversation and questioning them to know about the influence, behavioral changes caused on them by the social networking websites.

This research also involves the examination of - both participatory and directly methods, where directly examination was done with family members, friends, colleagues which help us to know some of the facts that was related to the analysis research[3]. The second method participatory examination was done by being active member in one or more social networking websites. While discussing the topics in forums, examination were made that helped in knowing about the information and facts related to the research.

V DATA ANALYSIS AND INTERPRETATIONS

Table: 1 - Purpose of Internet usage in India:

Uses	Percentage %
For E-Mail	30
For Surfing	25.8
For Chatting	22.7
Social Networking	18.0
Others	3.5
Total	**100**

The main use of Internet for mailing and surfing the internet with 30% and 25% respectively. Mailing and surfing internet are two common reasons for using Internet from times of Web 2.0.(Web technologies in 90s). In Indian youth, social networking websites are growing to gain momentum in its popularity and usage but have not yet reached the expectations matching the global scenario. Only 18% respondents reported social networking websites as their main purpose of Internet usage. The other responses were downloading content, buying goods online, studying andreading e-books[4].

Table: 2 - Membership in social networking websites:

Members of SNS	Percentage %
Yes	97.7
No	2.3
Total	**100**

A exceptional 97% of sample was member of one or more social networking websites which clearly makes a strong statement being a member in one or more social networking websites among Indian youth and teenagers. Breaking the data down further, almost 30% of the respondents were members of www.Orkut.com and 50% were in www.facebook.com[4] While other sites mentioned were Tagged,Netlog, MySpace, WAYN, Hi5, BigAdda, Linkedin, Stylefm, Twitter, Ning, Indyarocks, Friendster, and ebuddy.

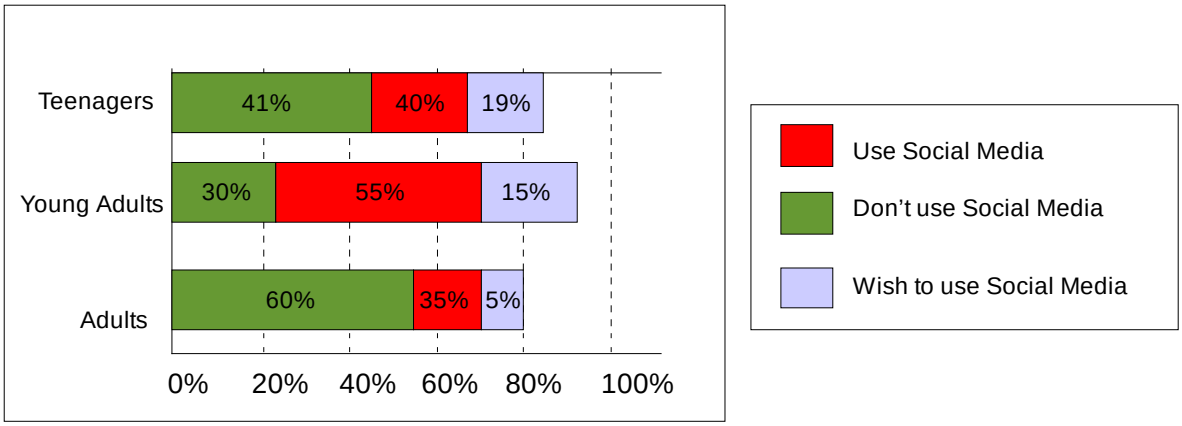
Table: 3 - Usage of social networking sites:

Hours	Percentage %

Less than 1 Hr.	78.1
1-2hrs	18.2
3-5 Hrs.	3.7
7-8 Hrs.	0.0
Total	**100**

In the above sample, hours were spent on social networking websites was less than1 hr for 78% of the respondents while there were no respondents using the social networking websites for more than 6 hrs. Moderate responses of about 18% use for 1-2hrs but a very low percentile of 3.7% uses it for 3-5hrs. Majority of the sample were exposed to social networking sites for shorter duration dueto various reasons such as no Internet connectivity at home, residing at hostelwith no Internet provisions or low level of interest in social networking sites.

According to one another survey it has been recorded the ratios of teenage users and students by categorizing the users in three categories one of which is teenagers (12 - 16) second one is young adults (17 – 21) and the third one is adults (22+)[1] as shown in figure 1.3.



As shown in figure 1.3 it has shown the ratios of teenage and students users with the average of using social networks, not using social networks and wishes to use social networks. Theaverage of users those who use social networks are those users which use social networks regularly on daily bases, while those users who wish to use social networks are those who don't have internet or parental permission or any other problem to use social networks but they wish to use social networks. It has been recorded anothercommunity of people those who don't use social networks in fact they don't want to use social networks because they dislike social networks.

VI IMPACT OF SOCIAL NETWORKS ON INDIAN EDUCATION

Education is important part of personal's life for every Indian students and teenager education is more important than anything[4]. Today students and teenagers are take interest for using social media but regrettably Social media Networks affect the Indian education badly. Above research has calculated that more than 85% of college students and teenagers use social media networks. Information Technology has fastly developed small communication devices but these small communication devices are basically used for accessing social media networks website any time anywhere, these communication devices are Tablets, iPhones, pocket computers, laptops, palm-tops, iPads and

even mobile phones also (which support internet). Information Technology is step towards advancement, no doubt but any technology which provide ease of social media can be harmful for social media followers. Social Networking sites grab the total concentration and attention of the Indian students & teenagers[4]. Social Media sites deflects them towards non educational, immoral and unsuitable actions like as useless chatting, time killing by unnecessary searching on internet. The social network sites addict becomes a useless node for parents, friends and other associated people. Social networking sites are use to support of difference implicit applications by virtue of which it grabs the attention of India students and increase the number of users. The Social media applications include advertisements, games, Entertainment and other online activities such as online video conferencing, live television etc. Social Media Users can use these applications free in there gazettes. All the Social Media applications are based on 2D and 3D screen play so by watching long time same display screen could cause high blood pressure and tension which could be risky for education as well as health also. According to social media analysis survey students do not take their lunch/dinner on time and do not sleep on proper timing which create a problem for students attitude with education. Social networks provide a virtual life to the Indian students, those students who not even speak in front of anyone could feel freedom in their virtual life. When they use social networking website they feel like in heaven but this addiction kills their inner self confidence for life time. The addiction of social media are going far from your friends, family, teachers and other associations could be very much dangerous for life and education. It changes the mind of Indian students completely like imagination. This virtual life of Indian students demolished his thoughts from education towards other activities and by living inside delusion world student slowly starts to hate educated life and studies. Social Media is the incident of understanding the other users by viewing their profiles, likes, comments, actions and other activities performed. In this regards opposite gender can be attracted by one another and to find faith of any friend all most each and every student spoils months and weeks on eavesdropping. According U.S. Military banned the use of social media websites in 2007 and Canadian government also banned social media websites for their employees in 2007 while U.S. Congress has decided to block such social media networking websites in schools, library and other educational institute[4]. Social networking websites expect a very negative effect of every peoples and age including teenagers, young adults and adults are regularly impress towards social networks, international and national jurisdiction must take action against social media networking websites.

VII CONCLUSIONS

The growth of social media sites shows an important change in Indian Students and teenagers behavior in their life. The social media websites has become an important part of our life today. It could extinct the future of Indian teenagers and children and it had a very bad effect on education as it is argue above. There is no other society or any third party which could check for what actions are been performed by which user, so it is strongly recommended to check teenager's activities on social media websites and don't let them use social networking websites. It is also a strong recommendation for international and Government cyber control to take part and ban these type of social networking websites[5], other than government and jurisdiction, every parents should closely banned the use of social networks on their children and secure their future.

REFERENCES

[1] N. Ellison, C. Steinfeld, C. Lampe, "Spatially bounded online social networks and social capital: The role of Facebook" In Proceedings from the annual conference of the international communication association. Dresden, Germany, June 2006.

[2] M. Asfandyar Khan1, "The Impact of Social Media and Social Networks on Education and Students of Pakistan", In Journal of Marketing, Vol. 73, Issue 5, page 90-102, September 2009.

[3] Danah M. Boyd & Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship", In Journal Of Computer-Mediated Communication, Vol. 13, Issue 1, October 2007.

[4] S. Kuppuswamy, P. B. Shankar Narayan, "The Impact of Social Networking Websites on the Education of Youth", In International Journal of Virtual Communities and Social Networking, Vol. 2, Issue 1, page 67-79, January-March 2010.

[5] Jeff Cain, "Pharmacy Students' Facebook Activity and Opinions Regarding Accountability and E-Professionalism" In American Journal of Pharmaceutical Education, Vol. 73, Issue 6, October 1, 2009. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2769526/