CLOUD COMPUTING AND SECURITY ISSUES

Rohini Dhage *

ABSTRACT

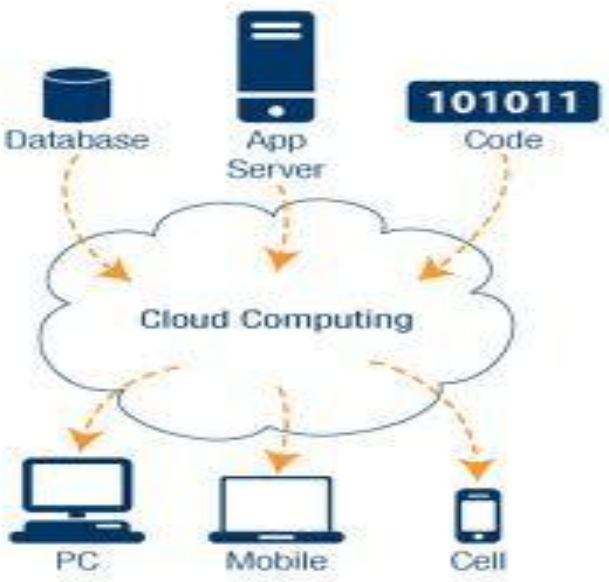
The field of cloud computing is still in its infancy as far as implementation and usage, partly because it is heavily promoted by technology advancement and is so high resource dependent that researches in academic institutions have not had many opportunities to analyze and experiment with it. In this paper, we discuss security issues for cloud computing and service providers for cloud. Given its recent development and scarcity of academic published work, many discussions on the topic of cloud security have surfaced from engineers in companies that provide the aforementioned services. Nevertheless, academia is developing in a significant presence, being able to address numerous issues.

Keywords: *Cloud Computing, Security, confidentiality, integrity and availability, Service SaaS, PaaS and IaaS.*

* PCD ICSR, VMV College Campus, Wardhaman Nagar, Nagpur, MS, India.

1. INTRODUCTION

Cloud computing has recently emerged as a new information technology infrastructure. Cloud computing has unique attributes that raise many security and privacy challenges in areas such as data security, recovery, and privacy, as well as legal issues in areas such as regulatory compliance and auditing. In contrast to traditional enterprise IT solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the servers in large data centers on the Internet, where the management of the data and services are not fully trustworthy. When clients store their data on the server without themselves possessing a copy of it, how the integrity of the data can be ensured if the server is not fully trustworthy? Will encryption solve the data confidentiality problem of sensitive data? How will encryption affect dynamic data operations such as query, insertion, modification, and deletion? Data in the cloud is typically in a shared environment alongside data from other clients. How the data segregation should be done, while data are stored, transmitted, and processed? Due to the fundamental paradigm shift in cloud computing, many security concerns have to be better understood, unanticipated vulnerabilities identified, and viable solutions to critical threats devised, before the wide deployment of cloud computing techniques can take place.

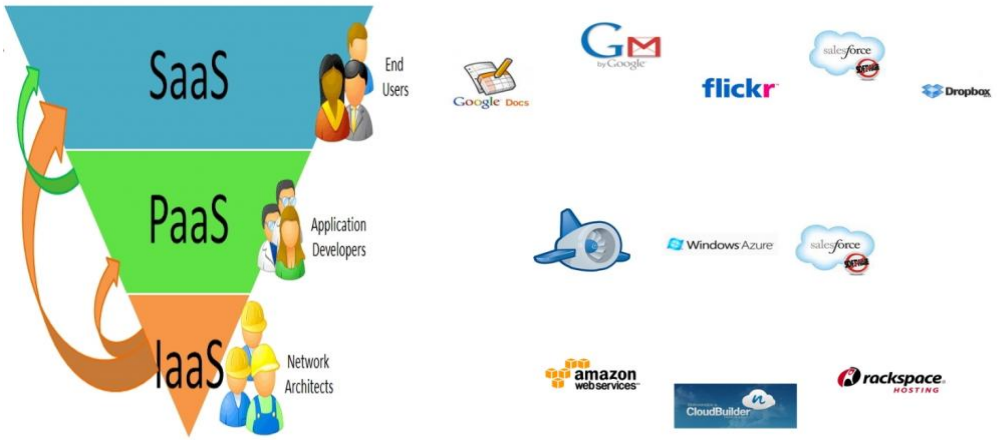


2. TYPES OF CLOUD PROVIDERS:

Cloud services are usually divided in the three main types, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

2.1 Software as a Service (SaaS)

SaaS clients rent usage of applications running within the Cloud‟s provider infrastructure, for example Sales Force. 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.



2.2 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.

2.3 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 virtualised platform and is not responsible for managing the underlying infrastructure.

3. CLOUD COMPUTING FUTURE:

Cloud computing is not an innovation, but a means to constructing IT services that use advanced computational power and improved storage capabilities. The main focus of cloud computing from the provider's view as extraneous hardware connected to support downtime on any device in the network, without a change in the users' perspective. Also, the users' software image should be easily transferable from one cloud to another. Balding proposes

that a layering mechanism should occur between the front-end software, middle-ware networking and back-end servers and storage, so that each part can be designed, implemented, tested and ran independent from subsequent layers. This paper introduces the current state of cloud computing, with its development challenges, academia and industry research efforts. Further, it describes cloud computing security problems and benefits and showcases a model of secure architecture for cloud computing implementation.

- **Convenience**

  Cloud computing allows people to access data and documents from any computer, tablet or smart phone, as long as they have a working internet connection. This is especially helpful when working on collaborative projects, as documents can be simultaneously viewed and edited from widely disparate locations. The automatic software updates that come with cloud software also make it easier to keep up with current regulations and compliance laws.

- **Cost**

  Cloud computing is more cost-effective than traditional software. Instead of purchasing and installing programs onto various devices, the software exists on a remote server. Use of the software is on a subscription basis rather than purchasing the software outright. In other words, businesses are required to pay for the service only when it is required. This saves money and provides the flexibility to scale up or down as demand fluctuates. For companies that have seasonal spikes, cloud computing provides a distinct advantage over buying software.

- **Storage**

  Another major benefit from utilizing the cloud is the doing away with server and hard drive constraints. Cloud computing businesses offer varying degrees of storage, and upgrading capacity is simply a matter of paying a higher monthly fee. Conversely, increasing storage space by traditional means would involve purchasing expensive equipment and installation costs. Maintenance expenditures are also eliminated as all the storage equipment is owned by the cloud computing provider. There is no need for a specialist IT staff to fix bugs and install upgrades relative to the software. An example of this type of storage is SugarSync.

- **Security and Backup**

  Cloud software cannot be pirated as the program is hosted on a single centralized server. These servers are extremely resilient and hosted over multiple countries, making it highly

unlikely that data will be lost or inaccessible. Moreover, the cost of security is defrayed as the provider is responsible for maintaining the integrity of the system. As the cloud computing provider's business is dependent on keeping client data secure, these measures are often complex and impossible to crack.

- **Green Credentials**

  In a recent study by Microsoft, cloud computing was purported to reduce carbon emissions for businesses by as much as 30 percent. This is primarily due to the energy savings garnered from utilizing the cloud in lieu of an entire in-house server. Going green saves your company money while at the same time can be used as an effective marketing strategy to clients looking for more responsible businesses.

So regardless of what reasons you use the Cloud just know that this type of storage and ways to interact with your data is the way of the future.

4. SECURITY CHALLENGES:

Start-up companies often lack the protection measures to weather off an attack on their servers due to the scarcity of resources - poor programming that explores software vulnerabilities (PHP, JavaScript, etc) open ports to firewalls or inexistent load-balance algorithms susceptible to denial of service attacks. For this reason, new companies are encouraged to pursue cloud computing as the alternative to supporting their own hardware backbone. However cloud computing does not come without its pitfalls. For starters, a cloud is a single point of failure for multiple resources. Even though network carriers such as AT&T believe a distributed cloud structure is the right implementation, it faces major challenges in finding the optimal approach for low power transmission and high network availability; some people believe that major corporations will shy away from implementing .Cloud solutions in the near future due to ineffective security policies. One problem comes from the fact that different cloud providers have different ways to store data, so creating a distributed cloud implies more challenges to be solved between vendors. cloud solutions in the near future due to ineffective security policies. One problem comes from the fact that different cloud providers have different ways to store data, so creating a distributed cloud implies more challenges to be solved between vendors.

4.1 Data Security:

Security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus,

the client company should own the encryption keys. Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervious to attacks based on capturing this data. However, companies have implemented systems with unpublished APIs, claiming that it improves security; unfortunately, this can be reversed engineered; also, using DHCP and FTP to perform tasks such as firmware upgrades has long been rendered as insecure. Nevertheless, products from Wyse are marketed with their thin client as one of the safest, by using those exact features.

Lastly, the most problematic issue is availability, as several companies using cloud computing have already experienced downtime (Amazon servers subject to what appeared to be a denial of service attack). Other things to keep in mind are contract policies between clients and vendors, so that data belongs only to the client at all times, preventing third parties to be involved at any point. Also, authentication should be backed by several methods like password plus flash card, or password plus finger print, or some combination of external hardware and password. One benefit of cloud computing is that client software security does not need to be enforced as strictly as before. This aspect concerns the view of cloud computing as software as a service, as it becomes more important to ensure security of data transfer rather than a traditional secure application life cycle.

4.2 Cloud Computing Security Issues:

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

Security issues are as follows:

- **Privileged user access -** information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water
- **Regulatory compliance -** clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't.
- **Data location -** depending on contracts, some clients might never know what country or what jurisdiction their data is located.
- **Data segregation -** encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.
- **Recovery -** every provider should have a disaster recovery protocol to protect user data
- **Investigative support -** if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation
- **Long-term viability -** refers to the ability to retract a contract and all data if the current provider is bought out by another firm, given that not all of the above need to be improved depending on the application at hand, it is still paramount that consensus is reached on the issues regarding standardization.

4.3 Security Benefits:

There are definitely plenty of concerns regarding the inability to trust cloud computing due to its security issues. However, cloud computing comes with several benefits that address data security. The following sections looks into addressing concepts such as centralized data, incident response or logging.

Centralized Data refers to the approach of placing all eggs in one basket. It might be dangerous to think that if the cloud goes down, so does the service they provide, but at the same time, it is easier to monitor. Storing data in the cloud voids many issues related to losing laptops or flash drives, which has been the most common way of loosing data for large enterprises or government organizations. The laptop would only store a small cache to interface with the thin client, but the authentication is done through the network, in the cloud. In addition to this, when a laptop is known to be stolen, administrators can block its

attempted access based on its identifier or MAC address. Moreover, it is easier and cheaper to store data encrypted in the cloud that to perform disk encryption on every piece of hardware or backup tape.

Incident Response refers to the ability to procure a resource such as a database server or supercomputing power or use a testing environment whenever needed. This bypasses the supplemental red tape associated with traditional requesting of resources within the corporate world. Also, if a server is down for re-imaging or disk clean-up, the client may easily create similar instances of their environment on other machines, improving the acquisition time. From a security standpoint, cloud providers already provide algorithms for generating hashes or checksums whenever a file is stored in the cloud, which bypasses the local/client need for encrypting. This does not imply that clients should not encrypt the data before sending it, but merely that the service is already in place for them.

Password Assurance Testing is a service that can be used to harness the computational power of the cloud in attempts to break into a company's system by guessing passwords. This approach minimizes resources and time spent on the client side. Logging benefits come from the idea that the client need not worry about storage space for log files and enjoys a faster way of searching through them. Moreover, it allows for a convenient way to observe which user accessed certain resources at any given time.

Improvement of Secure Software refers to several aspects in the development lifecycle of a product. Initially, a company that is thinking of placing their application in the cloud knows that the cost of running the application are directly proportional with the number of processing cycles, thus creating an incentive for an optimal implementation. Secondly, it becomes easier to monitor the effects of various security policies implemented in the software, without the overhead of traditional switching environments from development to production or to testing. Creating a new environment simply means creating a clone of the extant one. Thirdly, software run behind an architecture that is build for secure transactions at a physical, data link, network and transport layer, making it easier to design the application without the outspoken need of a security software engineer. Moreover, some cloud providers may use code scanning to detect vulnerabilities in the application code.

5. SUMMARY AND CONCLUSION:

In this paper, we first discussed actual what cloud computing is used in future ,types of cloud provider in cloud computing and its security issues for cloud. The main goal is to securely store and manage data that is not controlled by the owner of the data. Then we focused on

specific aspects of cloud computing. In particular, we are taking a bottom up approach to security where we are working on small problems in the cloud that we hope will solve the larger problem of cloud security.

6. REFERENCES

1. http://www.contextis.com/research/white-papers/assessing-cloud-node-security/Context- Assessing_Cloud_Node_Security-Whitepaper.pdf
2. cloud_computing/5%20Reasons%20Cloud%20Computing%20Is%20The%20Future%20%20%20Business%202%20Community.htm
3. [Weinberg08] Neil Wienberg, "Cloudy picture for cloud computing", 2008 http://www.networkworld.com/news/2008/043008-interop-cloud-computing.html?ap1=rcb
4. [Schwartz08] Ephraim Schwartz, "Hybrid model brings security to the cloud", 2008 http://www.infoworld.com/d/cloud-computing/hybrid-model-brings-security-cloud-364
5. [OCC08] The Open Cloud Consortium, 2008 http://www.opencloudconsortium.org/index.html
6. http://unix.nocdesigns.com/cloud_computing_white_paper.htm