ID: 2016-ISFT-151

A Review on the Evolution of Cloud Computing

Kajal Goel

Computer Science and Engineering at Maharaja Agrasen Institute of Technology, New-Delhi, India
kajal13goel@gmail.com

Abstract: *Cloud computing introduces a new era of IT opportunities and challenges. It is the latest technique of providing computational resources as a "service". The cloud is just a metaphor for the Internet. Cloud computing, often referred to as simply "the cloud", is the delivery of on-demand computing resources—everything from applications to data Centre's—over the Internet on a pay-for-use basis .It is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Many companies today are virtualizing their critical-applications. To do so they need the virtual machines associated with those applications to run on powerful and resilient servers. Cloud computing gives a way to do this without having to buy new servers. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. It is potential to be "greener" and "more economical" as average amount of energy needed for a computational action carried out in the cloud is far less than average amount for an on-site deployment. This is because different organizations can share the same physical resources securely, leading to more efficient use of the shared resources.In this paper I provide a comprehensive study on the features and incentives for adopting cloud computing in today's modern era followed by providing security, flexibility and ease over traditional IT service environment.* The study is to show cloud computing *as a general term for anything that involves delivering "hosted services" over the Internet and how these services are broadly divided into three categories of service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).It also include security issues associated with this technology and the possible measures that could be undertaken to solve it. The later includes technical challenges in cloud environment.[1]*

Keywords: *Cloud computing, cloud service, cloud security, computer network, distributed computing, security.*

1. INTRODUCTION

Traditional systems provide various kinds of benefits such as mature system functionality and abilities of greater customization and integration.The old guard of computing has been reversed. With increasing adoption of high-powered mobile devices and applications, more and more information is being created outside of centralized data centers and at ever increasing, rapidity.With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more available than ever before. This technological trend has enabled the realization of a new computing model called *cloud computing*. [2] Cloud computing means on demand delivery of IT resources via the internet with pay-as-you-go pricing.It is a modern trend that reveals the next-generation application architecture in which resources are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion.Cloud computing has the potential to radically change the nature of Information and Communication Technology (ICT) provision in public service and significantly reduce costs. It is the responsibility of cloud provider to manage resources and their performance. Management of resources includes several aspects of cloud computing such as load balancing, performance, storage, backups, capacity, deployment, etc. The management is essential to access full functionality of resources in the cloud. Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a web services API. The cloud computing market will rise from $40.7 billion this year to more than $241 billion in 2020, with a year-to-year growth of over 20 percent.

2. ANATOMY OF CLOUD COMPUTING

2.1 DEFINITION

"Cloud Computing is a form of IT-based capability – such as internet based services, software, or IT infrastructure – offered by a service provider that is accessible via internet protocols from any computer always available and scales automatically to adjust the demand,is either pay-per-use or advertising –based, has Web or programmatic-based control interfaces, and enables full customer self-service." In cloud computing, the phrase "the cloud" is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different servicessuch as servers, storage and applicationsare delivered to an organization's computers and devices through the Internet. It

relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth.A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider. This technological trend has enabled the realization of a new computing model, in which resources are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. Five key attributes of cloud computing are broad network access, rapid elasticity, measured service/Pay as you go, on demand self-service, Resource pooling.

2.2 CLOUD COMPUTING ARCHITECTURE

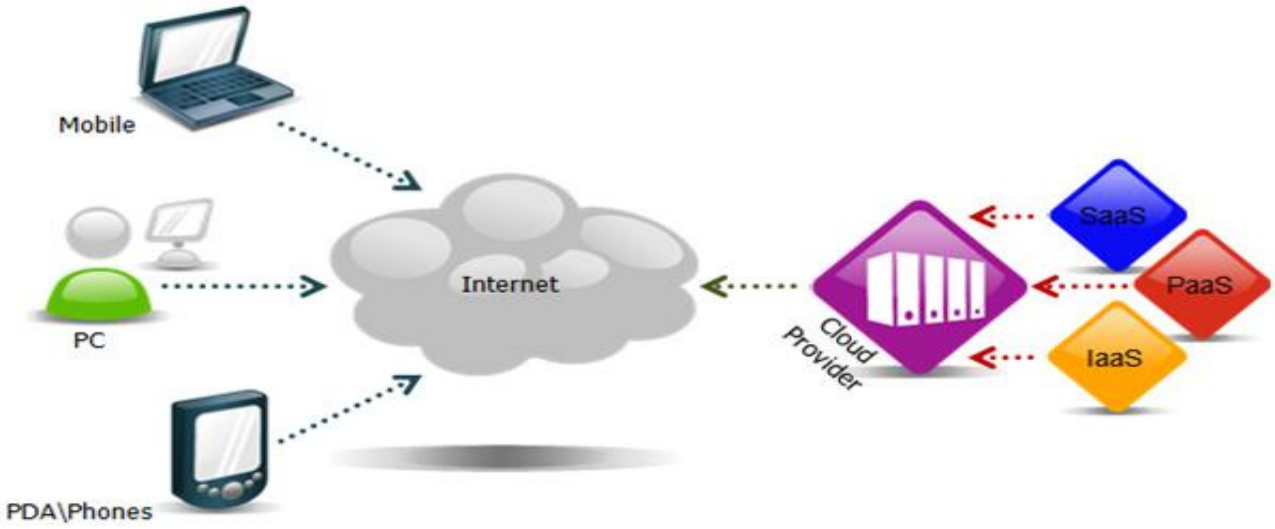

Fig. 1.CLOUD COMPUTING ARCHITECTURE

2.3 CLOUD SERVICE MODEL

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [3]

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. *It provides run time environment to create web applications. [3]*

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). *[3]*

2.4 CLOUD DEPLOYMENT MODEL

Public Cloud: A public cloud is established where several organizations have similar requirements and seek to share infrastructure so as to appliance. In addition, it can be economically attractive as the resources (storage, workstations) utilized and shared in the community are already exploited. This is the cloud computing model where service providers make their computing resources available online for the public. It allows the users to access various important resources on cloud, such as: Software, Applications or Stored data. [3]

Community Cloud: Community cloud shares infrastructure between several organizations from a specific community with common concerns, whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than that of a private) to realize its cost saving potential. [3]

Private Cloud: Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow

businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. [3] It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally.

Hybrid Clouds: these are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models.[3] In a hybrid cloud, you can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

2.5 CLOUD COMPUTING SECURITY

The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. [4] One of the most important aspects refers to security. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution. It indicates a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing. These concerns have their origin not only on existing problems, directly inherited from the adopted technologies, but are also related to new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization (e.g., data leakage and hypervisor vulnerabilities). [5]We identify the main problems in the area and group them into a model composed of seven categories, namely, the categories are: network security, interfaces, data security, virtualization, governance and compliance.

Fig. 2. Cloud computing security

2.6 CLOUD COMPUTING SECURITY ISSUES

1. **Network Security:** Problems associated with network communications and configurations regarding cloud computing infrastructures. Transfer security having distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks. Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders. They also enable VM isolation, fine-grained filtering for addresses and ports and detection of external security assessment procedures. Security configuration includes configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency. [4]

2. **Interfaces:** Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds. API having programming interfaces (essential to IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use. Administrative interface enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations). User interface: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment. For authentication mechanisms are required to enable access to the cloud.

3. **Data security:** Protection of data in terms of confidentiality, availability and integrity. Cryptography, most employed practice to secure sensitive data, thoroughly required by industry, state and federal regulations. Redundancy essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes and, thus, mission-critical data integrity and availability must be ensured. Disposal having elementary data disposal techniques which are insufficient and commonly referred as deletion .In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement. [4]

4. **Virtualization:** Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies. Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM. Data leakage exploits hypervisor vulnerabilities and lack of

isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity. Cross-VM attacks include attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks. One example consists in overlapping memory and storage regions initially dedicated to a single virtual machine, which also enables other isolation-related attacks. [4]

5. **Privacy:** It is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. [5]

6. **Governance:** Issues related to (losing) administrative and security controls in cloud computing solutions. Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations needs data control. Security control is required to loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps. [4]

7. **Compliance:** Includes requirements related to service availability and audit capabilities. Mechanisms to ensure the required service availability and the basic security procedures to be adopted required service level agreements. Loss of service outages is not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS). Audit allows security and availability assessments to be performed by customers, providers and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions. [4]

2.7 GENERAL SECURITY COUNTERMEASURES

1. **Architecture security:** Cloud computing security challenges can be handled practically by performing security. The architecture of cloud includes various security components like Access Management, Security API, Network Security and Storage Security. These components embedded in the cloud architecture to provide secure cloud computing. [5]

2. **Data Security:** Privacy in terms of legal compliance and user trust, data leakage for sensitive data are provided. Ji Hu Klein gave a benchmark to secure data-in-transit in the cloud. Cloud computing attacks are discussed and some provisions and means to overcome from the same are proposed. Jensen et al give the foundations of technical Security issues which consist of web service security using XML and SOAP messages, and Transport Layer security using SSL.[5]

3. **Using Client Based Privacy Manager:** Client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacy related benefits. The main features of the privacy manager are Obfuscation, that automatically obfuscate some or all of the fields in a data structure before it is sent off. [5]

4. **Security Concerns with the Hypervisor:** If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor. Based on the understanding of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs (Virtual Machines) and inter-communication among the various infrastructure components.[4]

5. **Sniffer Attacks:** A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

6. **Better Enterprise Infrastructure:** Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks. [5]

7. **Confronting Data Loss/Leakage:** To confront this threat, one should implement strong API access control. Another effective measure is to Encrypt and protects integrity of data in transit, and Analyze data protection at both design and run time. Other good steps to take are to Implements strong key generation, storage and management, and destruction practices, and Contractually demand providers to wipe persistent media before it is released into the pool. The manager can also contractually specify provider backup and retention strategies. [5]

3. CONCLUSIONS

Cloud computing have several benefits over traditional (non- cloud) environment and have capability to handle most sudden, temporary peaks in application demand on cloud infrastructures. Virtualization technology provides good support to achieve aim of cloud computing like higher resource utilization, elasticity, reducing IT cost or capital expenditure to handle temporary loads as well as cloud computing have various flexible service and deployment models which is also one of the main issue of adopting this

computing paradigm. [6]Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. So there is need to focus on privacy and on solutions of various security problems to maintain the trust level of organization for deploying the cloud computing without any hesitation and also need of technical support for elastic scalability to serve by vertical scaling approach which is currently restricted to only horizontal scaling.The social implications of cloud computing approaches might emerge with severe impact if robust security models for cloud computing do not exist. Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require to analyze the practicality in line with social, business, technical and legal perspectives – all these facets will incorporate security issues either in technical or strategic form. Regardless of the nature of security issues, it can be undoubtedly concluded that the severe adverse effects as a consequence of security breaches in cloud computing, the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems. [7]

REFERENCES

[1] Nandgaonkar, S.; Raut, A. B. A Comprehensive Study on Cloud Computing. International Journal Of Computer Science and Mobile Computing, Vol. 3, Issue. 4, April 2014, pg.733 – 738.

[2] Duan, J.; Faker, P.; Fesak, A.; Stuar, T. Benefits and Drawbacks of Cloud-Based Versus Traditional ERP Systems. Tilburg University, TiSEM.

[3] NIST Definition of Cloud Computing - Service architecture. The NIST Definition of Cloud Computing.

[4] Tiwari, P.; Mishra, B.; Cloud Computing Security Issues, Challenges and Solution. International Journal Of Emerging Technology and Advanced Engineering, 2012 Volume 2, Issue 8.

[5] Ashktorab, V.; Taghizadeh, S.R. Security Threats and Countermeasures in Cloud Computing. International Journal Of Application or Innovation in Engineering & Management, 2012, Volume 1, Issue 2.

[6] Gonzalez, N.; Miers, C.; Red´ıgolo, F.; Simpl´ıcio, M. et al. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. Journal of Cloud Computing.

[7] Ahmed, M.; Hossain, M.A. Cloud Computing and Security Issues in the Cloud. International Journal of Network Security & Its Applications (IJNSA), 2014, Vol.6, No.1.