A Review Paper on Cloud Computing

Er. Varun Sharma[1]
[1]Department of Information Technology
[1]IET BhaddalRopar

Abstract— Cloud computing is the biggest buzz in the computer world these days—maybe too big of a buzz. Cloud computing presents a new model for IT service delivery and it typically involves over-a-network, on-demand, self-service access, which is dynamically scalable and elastic, utilizing pools of often virtualized resources. It’s important to make clear at the outset that cloud computing in the developing world is in its infant stage. In this paper we review various aspects of cloud computing like its existing architectures, its benefits along with its security, trust and privacy issues.

Key words: Cloud Computing, Benefits, Issues, Security

I. INTRODUCTION

During the 1990s, data center floor space, power, cooling and operating expenses increased and lead to the adoption of grid computing and virtualization. Through grid computing users could plug in and use a metered utility service. By allowing the infrastructure to be virtualized and shared across consumers, service providers needed to change their business model to provide for remotely managed services and lower costs. As services became more and more distributed, a need for integration and management of these services became important and lead to the emergence of service-oriented architecture (SOA). Cloud computing developed out of this need to provide IT resources ‘as-a-service’.[1]

A cloud may be thought of as a large pool of resources, unified through virtualization or job scheduling techniques; these resources can be managed to dynamically scale up to match the load, using a pay-per- resources business model. These resources are made available through a new cloud computing paradigm that is being increasingly adopted by organizations; the resources include hardware and systems software on remote datacenters, as well as services based upon these that are accessed through the Internet. Key features advertised are elasticity, multi-tenancy, maximal resource utilization and pay-per-use. These new features provide the means to leverage large infrastructures like data centers through virtualization or job management and resource management, but these large pools of resources are not necessarily located in the same country nor even on the same continent. Furthermore, the dynamic expansion or shrinkage of a cloud makes it difficult to keep track of what resources are used and in which country. This makes compliance with regulations related to data handling difficult to fulfill. Auditing is also a challenging task due to the volatility of the resources used. These new features make it hard – and sometimes not possible at all – to reuse traditional security, trust and privacy mechanisms in the cloud. Moreover they raise issues and concerns that need to be fully understood and addressed. Some of these issues will be shared with other paradigms, such as service- oriented architectures (SOA), grid, web-based services or outsourcing, but often they are exacerbated by cloud. [2]

II. BACKGROUND

The IT environment evolved from mainframes to client servers, the Internet, virtualization and cloud computing. Cloud computing provides a shared pool of configurable IT resources (e.g. processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, on a measured (pay-per-use or subscription) basis, which needs minimal management effort, is based on service level agreements between the service provider and consumers, and often utilizes virtualization resources. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if it was a program installed locally on their own computer. Cloud computing can include software (software-as- a-service), hardware (infrastructure-as-a-service), or technology tools (platform-as-a-service) that are available on demand, as opposed to licensed software and tools, or purchased hardware. The type and quality of service and cloud computing requirements are, in most cases, agreed upon in a service level agreement (SLA) between the service provider and consumers. [1]

Virtualization technologies are one of the important building blocks in Cloud Platform Architectures. The dynamic infrastructure enabled by technologies such as virtualization aligns well with the dynamic on-demand nature of clouds. At a fundamental level, virtualization technology enables the abstraction or decoupling of the application payload from the underlying physical resource. What this typically means is that the physical resource can then be carved up into logical or virtual resources as needed. This is known as provisioning. By introducing a suitable management infrastructure on top of this virtualization functionality, the provisioning of these logical resources could be made dynamic, i.e., the logical resource could be made bigger or smaller in accordance with demand. This is known as dynamic provisioning. To enable a true “cloud” computer, every single computing element or resource should be capable of being dynamically provisioned and managed in real-time.[3]

III. CLOUD COMPUTING ARCHITECTURE

Cloud computing architectures are essentially subdivided into Cloud Platform Architecture (CPA) and Cloud Application Architecture (CAA) which are linked via the cloud services available on the marketplace of IT utilities. Such a division between CPA and CAA is fundamental for cloud computing to serve as a potential foundation for delivering IT services as utilities over the Internet, because by this way, the concerns of CSPs and CSCs are profoundly separated. Our elaborations on the constructs of CPA and CAA have manifested that while the focus of CPA lies at Internet-centric virtualization of IT capabilities and the elasticity, the focus of CAA is at service management and

SOAs, which will be able to provide a robust cloud computing environment despite heterogeneity and dynamic changes of CSPs. [3]

IV. CLOUD COMPUTING BENEFITS

Cloud computing provides compelling savings in IT related costs including lower implementation and maintenance costs; less hardware to purchase and support; the elimination of the cost of power, cooling, floor space and storage as resources are moved to a service provider; a reduction in operational costs; and paying only for what is used (measured service). Cloud computing also enables organizations to become more competitive due to flexible and agile computing platforms, providing for scalability and high-performance resources and highly reliable and available applications and data. Through cloud computing, IT departments save on application development, deployments, security, and maintenance time and costs, while benefiting from economies of scale. 'Going green' and saving costs are a key focus point for organizations. Cloud computing helps organizations to reduce power, cooling, storage and space usage and thereby facilitates more sustainable, environmentally responsible data centers. Moving to the cloud further frees up existing infrastructure and resources that can be allocated to more strategic tasks. [1]

V. CLOUD COMPUTING SECURITY CONCERNS

Although cloud computing's benefits are tremendous, security and privacy concerns are the primary obstacles to wide adoption.2 Because cloud service providers (CSPs) are separate administrative entities, moving to the commercial public cloud deprives users of direct control over the systems that manage their data and applications. Even if CSPs' infrastructure and management capabilities are much more powerful and reliable than those of personal computing devices, the cloud platform still faces both internal and external security and privacy threats, including media failures, software bugs, malware, administrator errors and malicious insiders.[4]

At the broadest level (and particularly from a European standpoint), privacy is a fundamental human right that encompasses the right to be left alone. In the commercial, consumer context, privacy entails the protection and appropriate use of the personal information of customers, and the meeting of expectations of customers about its use. For organizations, privacy entails the application of laws, policies, standards and processes by which Personally Identifiable Information (PII) of individuals is managed. [2]

An adequate risk mitigation strategy needs to be developed and followed to ensure mitigation of security risks and subsequent protection of data and applications in the cloud. Proper safeguarding and protection of valuable business data and systems remains the responsibility of management, regardless of whether or not the data and systems are hosted in the cloud.

In traditional security models, a security perimeter is set up to create a trust boundary within which there is self- control over computing resources and where sensitive information is stored and processed. For example, the corporate firewall often marks this boundary. The network provides transit to other trusted end hosts, which operate in a similar manner. This model held for the original Internet, but does not for public and hybrid cloud (a mixture between public and private deployment). The security perimeter becomes blurred in the sense that confidential information may be processed outside known trusted areas as these computing environments often have fuzzy boundaries as to where data is stored and/or processed. On the other hand, in order to obtain the service, consumers need to extend their trust to the cloud service provider, and so this can provide a point of friction.[2] Security and privacy is one fundamental obstacle to cloud computing's success. Clearly, much work remains for a trustworthy public cloud environment to become a reality.

VI. CONCLUSION

Cloud computing is a new technology widely studied in recent years. Now there are many cloud platforms both in industry and in academic circle. How to understand and use these platforms is a big issue.Though each cloud computing platform has its own strength, one thing should be noticed is that no matter what kind of platform there is lots unsolved issues. For example, continuously high availability, Performance, Data Confidentiality and Auditability, Synchronization in different clusters in cloud platform, interoperation and standardization, the security of cloud platform. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has a bright future.

REFERENCES

[1] Carroll, M., Merwe, A.V.D., Kotze, P., "Secure Cloud Computing", ISSA, pp. 1-9, August 2011.
[2] Pearson, S. and Benameur, A., "Privacy, Security and Trust Issues Arising from Cloud Computing", ICCCTS, pp. 693-702, 2010.
[3] Tianfield H., "Cloud Computing Architectures", IEEE, pp. 1394-1399, 2011.
[4] KuiRen, Cong Wang, and Qian Wang, "Security Challenges for the Public Cloud", IEEE Computer Society, pp. 69-73, 2012.
[5] Behl, A.,"Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation", WICT 2011, pp. 217 – 222, December 2011.
[6] Grobauer, B. Walloschek, T. and Stocker, E., "Understanding Cloud Computing Vulnerabilities", IEEE Security & Privacy, Volume-9, Issue-2, pp. 50-57, March-April 2011.
[7] Kaufman, L.M., "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Volume-7, Issue-4, pp. 61 – 64, July-August 2009.