Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 2, 2020

Review Article

EFFECTIVE IMPLEMENTATION OF LARGE-SCALE DATABASES AND CLOUD TECHNOLOGIES IN INDUSTRY

Ruziev Abdumalik Ortikalievich[1], Matniyazov Rakhim Rajabbaevich[2], Asraev Umar Muminovich[3]

[1]Senior lecturer, Department of Electronic Commerce and Digital Economics, Tashkent Financial Institute, Uzbekistan.
[2]Senior lecturer, Department of Electronic Commerce and Digital Economics, Tashkent Financial Institute, Uzbekistan.
[3]Senior lecturer, Department of Electronic Commerce and Digital Economics, Tashkent Financial Institute, Uzbekistan.
E-mail address: ruziyev56@gmail.com

Received: 15.11.2019 *Revised: 21.12.2019* *Accepted: 22.01.2020*

Abstract
In the last two decades, the continuous increase of computational power has produced an overwhelming flow of data. Moreover, the recent advances in Web technology has made it easy for any user to provide and consume content of any form. This has called for a paradigm shift in the computing architecture and large scale data processing mechanisms. Cloud computing is associated with a new paradigm for the provision of computing infrastructure. This paradigm shifts the location of this infrastructure to the network to reduce the costs associated with the management of hardware and software resources. This paper gives a comprehensive survey of numerous approaches and mechanisms of deploying data-intensive applications in the cloud which are gaining a lot of momentum in both research and industrial communities. We analyze the various design decisions of each approach and its suitability to support certain classes of applications and end-users. A discussion of some open issues and future challenges pertaining to scalability, consistency, economical processing of large scale data on the cloud is provided. We highlight the characteristics of the best candidate classes of applications that can be deployed in the cloud. Index Terms-Cloud Compu.

Key words. Cloud, provider, service, industrial, infrastructure services, cloud Service, business requirements.

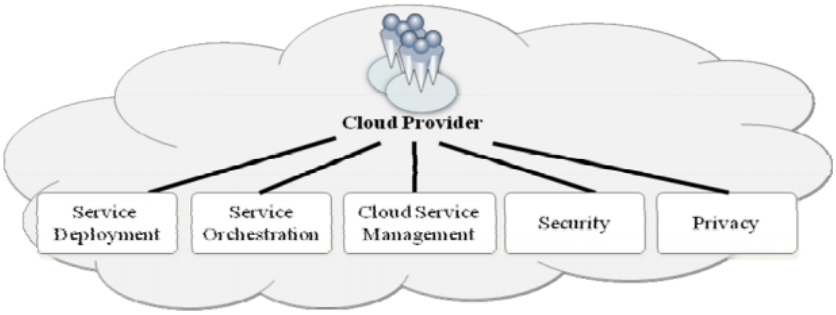
DOI: http://dx.doi.org/10.31838/jcr.07.02.56

INTRODUCTION

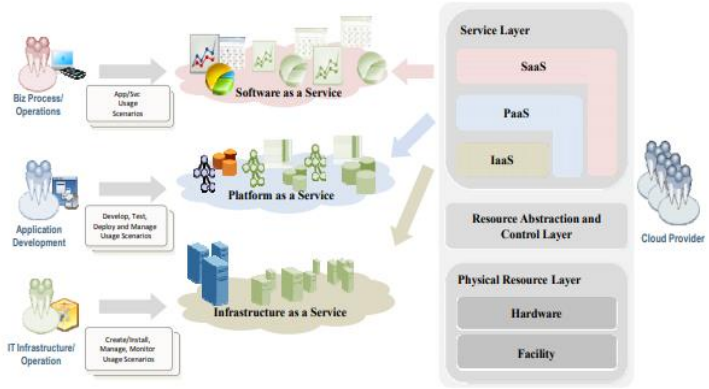
A cloud provider can be a person, an organization, or an entity responsible for making a service available to cloud consumers. A cloud provider builds the requested software/platform/ infrastructure services, manages the technical infrastructure required for providing the services, provisions the services at agreed-upon service levels, and protects the security and privacy of the services. As illustrated in Table 2, cloud providers undertake different tasks for the provisioning of the various service models. For Cloud Software as a Service, the cloud provider deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers.

MATERIALS AND METHODS

The provider of SaaS assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications. For Cloud Platform as a Service, the cloud provider manages the cloud infrastructure for the platform, and provisions tools and execution resources for the platform consumers to develop, test, deploy, and administer applications. Consumers have control over the applications and NIST Cloud Computing Standards Roadmap NIST SP500-291-v1.0 20 possibly the hosting environment settings, but cannot access the infrastructure underlying the platform including network, servers, operating systems, or storage. For Cloud Infrastructure as a Service, the cloud provider provisions the physical processing, storage, networking, and other fundamental computing resources, as well as manages the hosting environment and cloud infrastructure for IaaS consumers. Cloud consumers deploy and run applications, have more control over the hosting environment and operating systems, but do not manage or control the underlying cloud infrastructure (e.g., the physical servers, network, storage, hypervisors, etc.). The activities of cloud providers can be discussed in greater detail from the perspectives of Service Deployment, Service Orchestration, Cloud Service Management, Security and Privacy



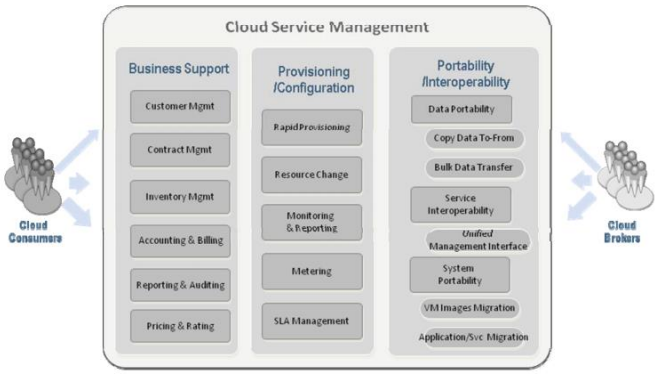
Service Orchestration Service orchestration refers to the arrangement, coordination, and management of cloud infrastructure to provide different cloud services to meet IT and business requirements. Figure 4 shows the general requirements and processes for cloud providers to build each of the three service models.



A three-layered framework is identified for a generalized cloud environment in Figure 4. The top layer is the service layer, where a cloud provider defines and provisions each of the three service models. This is where cloud consumers consume cloud services through the respective cloud interfaces. The middle layer is the resource abstraction and control layer. This layer contains the system components that a cloud provider uses to provide and manage access to the physical computing resources through software abstraction. The layer typically includes software elements such as hypervisors, virtual machines, virtual data storage, and other resource abstraction and management components needed to ensure efficient, secure, and reliable usage.

RESULT AND DISCUSSION

While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded. This layer provides "cloud readiness" with the five characteristics defined in the NIST definition of cloud computing. The lowest layer in the framework is the physical resource layer, which includes all the physical computing resources. This layer includes hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links, and interfaces), storage components (hard disks), and other physical computing infrastructure elements. It also includes facilities resources, such as heating, ventilation, and air conditioning (HVAC), power, communications, and other aspects of the physical plant. Note that in this framework, the horizontal positioning of layers implies a stack in which the upper layer has a dependency on the lower layer. The resource abstraction and control layer build virtual cloud resources on top of the underlying physical resource layer and support the service layer where cloud services interfaces are exposed. The three service models can be built either on top of one another (i.e., SaaS built upon PaaS and PaaS built upon IaaS) or directly upon the underlying cloud infrastructure. For example, a SaaS application can be implemented and hosted on virtual machines from IaaS or directly on top of cloud resources without using IaaS. Cloud Service Management. Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in Figure 5, cloud service management can be described from the perspective of business support, provisioning and configuration, and from the perspective of portability and interoperability requirements.



A cloud auditor is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of a cloud implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. Auditing is especially important for federal agencies as "agencies should include a contractual clause enabling third parties to assess security controls of cloud providers" (by Vivek Kundra, Federal Cloud Computing Strategy, February 2011.). Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system.

CONCLUSION

The security auditing should also include the verification of the compliance with regulation and security policy. Federal agencies should be aware of the privacy concerns associated with the cloud computing environment where data are stored on a server that is not owned or controlled by the federal government. Privacy impact auditing can be conducted to measure how well the cloud system conforms to a set of established privacy criteria. A privacy impact audit can help federal agencies comply with applicable privacy laws and regulations governing an individual's privacy, and to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation.

REFERENCES

1. T. Hey, S. Tansly, and K. Tolle, editors. The Fourth Paradigm: DataIntensive Scientific Discovery. Microsoft Research, October 2009.
2. G. Bell, J. Gray, and A. Szalay. Petascale computational systems. IEEE Computer, 39(1):110–112, 2006.
3. Massimo Lamanna. High-Energy Physics Applications on the Grid. In Lizhe Wang and Wei Jie and Jinjun Chen, editor, Grid Computing: Infrastructure, Service, and Applications, pages 433–458. CRC Press, 2009.
4. Yehia El khatib and Christopher Edwards. A Survey-Based Study of Grid Traffic. In GridNets '07, pages 4:1–4:8, 2007.
5. Daniel M. Batista, Luciano J. Chaves, Nelson L. S. da Fonseca, and A. Ziviani. Performance Analysis of Available Bandwidth Estimation Tools for Grid Networks. Journal of Supercomputing, 53:103–121, July 2010.
6. Gartner. Gartner top ten disruptive technologies for 2008 to 2012. Emerging trends and technologies roadshow, 2008.
7. M. Armbrust, A. Fox, G. Rean, A. Joseph, R. Katz, A. Konwinski, L. Gunho, P. David, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley View of Cloud Computing, Feb 2009.
8. L. Gonzalez, L. Merino, J. Caceres, and M. Lindner. A Break in the Clouds: Towards a Cloud Definition. Computer Communication Review, 39(1), 2009.
9. D. Plummer, T. Bittman, T. Austin, D. Cearley, and D. Smith. Cloud computing: Defining and describing an emerging phenomenon. Technical report, Gartner, June 2008.
10. J. Staten, S. Yates, F. Gillett, W. Saleh, and R. Dines. Is cloud computing ready for the enterprise? Technical report, Forrester Research, March 2008.
11. P. Mell and T. Grance. Definition of cloud computing. Technical report, National Institute of Standard and Technology (NIST), July 2009.
12. D. Parkhill. The challenge of the computer utility. Addison-Wesley, 1966.
13. Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-theart and research challenges. J. Internet Services and Applications, 1(1), 2010.
14. Kernal based virtual machine. www.linux-kvm.org.
15. Vmware esx server. www.vmware.com.
16. Xensource inc. www.xensource.com.
17. Ibrahim W. Habib, Qiang Song, Zhaoming Li, and Nageswara S. V. Rao. Deployment of the GMPLS control plane for grid applications in experimental high-performance networks. IEEE Commun. Mag., 44(3):65–73, 2006.
18. Thomas Lehman, Jerry Sobieski, and Bijan Jabbari. DRAGON: a framework for service provisioning in heterogeneous grid networks. IEEE Commun. Mag., 44(3):84–90, 2006.
19. Wei Guo, Weiqiang Sun, Yaohui Jin, Weisheng Hu, and Chunming Qiao. Demonstration of Joint Resource Scheduling in an Optical Network Integrated Computing Environment. IEE Communications Magazine, 48(5):76–83, 2010.
20. I. Foster, Y. Zhao, I. Raicu, and S. Lu. Cloud C
21. Kuni Zu'aimah Barikah. "Traditional and Novel Methods for Cocrystal Formation: A Mini Review." Systematic Reviews in Pharmacy 9.1 (2018), 79-82. Print. doi:10.5530/srp.2018.1.15