Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/67

A Quick Overview of Cloud-Based Services

Devesh Pratap Singh[1], Surendra Shukla[2], Dibyahash Bordoloi[3]

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University,
Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering,Graphic Era Deemed to be University,
Dehradun, Uttarakhand India, 248002
[3]Head of the Department, Department of Computer Science & Engineering,Graphic Era Hill
University, Dehradun, Uttarakhand India, 248002

ABSTRACT

In the realm of Services Computing, Cloud Computing has developed into a scalable platform for the consumption and delivery of such services. Service-oriented architecture (SOA) and virtualizations of hardware and software are the technological underpinnings of cloud computing. To determine the contours of a new age, we look to the evolution of technologies like cloud computing, which combines parallel and distributed processing, grid computing, and virtualization. Businesses are beginning to use cloud computing as a new method of data storage and management. In this study, we examine the architecture of the cloud and draw parallels between cloud and grid computing. In addition, we discuss the features and potential uses of various widely used cloud computing systems. The purpose of this study is to highlight some of the problems and difficulties associated with cloud computing. We found many obstacles from an adoption of cloud computing perspective and emphasised the cloud interoperability problem that needs considerable additional study and development. However, customers face significant resistance to adopting cloud computing systems due to concerns about security and privacy. In this research, we look at the worries of various cloud computing system vendors about security and privacy.

The purpose of cloud computing is to enable resource sharing amongst cloud service users, cloud partners, and cloud suppliers. Infrastructure cloud (e.g., hardware, IT infrastructure management), software cloud (e.g., SaaS focusing on middleware as a service, or traditional CRM as a service), application cloud (e.g., Application as a Service, UML modelling tools as a service, social network as a service), and business cloud (e.g., Software as a Service, UML modelling tools as a service, social network as a service) are all the result of resource sharing at different (e.g., business process as a service).

Keywords: Cloud Computing, Virtualization, Data recovery, Service provider.

INTRODUCTION

Cloud computing is a relatively new technology that provides customers with a pay-as-you-go paradigm for accessing computer resources including infrastructure, storage, software, and deployment environments [1]. Due to the dynamic and multi-tenant nature of the cloud environment, traditional digital forensics cannot manage the many technological, legal, and organisational difficulties that are unique to cloud systems. With cloud computing's adaptability comes a wealth of possibilities for conducting digital investigations on the cloud. Sharing resources between cloud service users, cloud partners, and cloud suppliers is fundamental to the concept of cloud computing. Infrastructure cloud (hardware, IT infrastructure management), software cloud (SaaS focusing on middleware as a service, or traditional CRM as a service), application cloud (Application as a Service, UML modelling tools as a service, social network as a service), and business cloud are all products of resource sharing at different levels (e.g., business process as a service) [2]. This article discusses the difficulties of doing digital forensics in the cloud, as well as some of the solutions currently available.

STRUCTURAL ELEMENTS

SaaS, PaaS, and IaaS are the three main categories used to categorise the various cloud service types.

SaaS, or "Software as a Service" (SaaS)

The Software as a Service (SaaS) concept is a way of delivering software to end users by having the service itself delivered to them through the Internet [3]. While Saas frees users from the tedium of software upkeep and support, it also requires them to give up some say in the program's versioning and other configuration settings. Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are two common phrases in this field (IaaS)

Service Platform as a Utility (PaaS)

Providers let users install their own or third-party applications built using languages, libraries, services, and tools supported by the provider into the cloud's infrastructure. Customer has authority over installed programmes and optionally configuration settings for the application hosting environment, but has no authority over the underlying cloud infrastructure such as network, servers, operating systems, or storage [4]. The service provider's responsibilities in a PaaS setting include not just the supply and management of lower-level infrastructure resources, but also the provisioning and management of a whole managed application development and deployment platform. PaaS often operates in a multitenant setting, providing developers with access to a wide variety of operating systems, databases, middleware, software tools, and managed services. With PaaS, developers are freed from worrying about infrastructure-level concerns like scalability, security, and more so that they can concentrate on what they do best: quick development and deployment.

IaaS

This is the gear that supports the software, and it includes things like networks, storage, and computers. IaaS paved the way for companies to better control Also hardware expenses, but it presented a difficult position for developers. During development and testing, developers are increasingly accountable for a greater share of operational tasks [5]. Hardware resource provisioning, configuration, management, and updates are all new skills they need to learn.

DAS, or Data as a Service (DaaS)

An whole new kind of Cloud service emerges: the data storage service, which provides virtualized storage on demand. Notably, DaaS may be seen as a subset of Infrastructure as a Service. This is due to the high initial investment required for on-premise business database systems, which typically includes a dedicated server, software licencing, post-delivery services, and in-house IT support. DaaS shifts the burden of licencing databases off of the shoulders of individual users by charging only for the data that is accessed [6]. Some DaaS offerings, in addition to RDBMS and file systems, provide table-style abstractions that are built to scale out to store and retrieve a huge amount of data within a very compressed timeframe; this amount of data is typically too large, too expensive, or too slow for most commercial RDBMS to deal with. Storage as a Service (DaaS) platforms like Amazon S3, Google BigTable, Apache HBase, etc.

A REVIEW OF THE DIFFERENCES BETWEEN THE CLOUD AND THE GRID

While cloud computing is designed to accommodate a wide variety of uses, there is currently no dedicated grid infrastructure for certain fields (such as biology, geography, or education) and this is what makes grid construction distinct from cloud computing.

2) Grid places an emphasis on "resource sharing" to create an online group. In most cases, a single physical entity (with the exception of community Cloud, which is owned by the community) manages the allocation of cloud resources to several instances [7].

(3) By pooling available resources, Grid attempts to ensure that even the most demanding of tasks may be completed with sufficient speed and efficiency. Cloud computing is designed to meet the needs of numerous low- and medium-volume jobs in real time. As a result, the idea of several tenants sharing a single Cloud resource is crucial.

4) In exchange for (research) high speed computing, Grid sacrifices reusability. The demand for cloud computing is driven directly by end users. Grid's ultimate goal is to maximise processing power. The goal of the cloud is on-demand computing, which allows for infinite scalability in terms of both resources and user demand [8].

Common Cloud Computing Environments.

AbiCloud A cloud computing platform, Abicloud may be used to construct, integrate, and control both public and private clouds in similar settings. Abicloud makes it simple and straightforward to set up and administer infrastructure components including servers, storage, networks, virtual machines, and software. With its robust web-based administration function and fundamental encapsulation approach, Abicloud stands apart from competing cloud computing solutions. The Abicloud makes it possible to install a new service with the click of a mouse. Compared to other cloud computing platforms, where new services are deployed through command lines, this method is both simpler and more adaptable.

Eucalyptus

Open source private cloud infrastructure was mostly constructed using Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) . It is an open-source, cluster- or workstation-based implementation of elastic, utility, cloud computing and a widely adopted computing standard based on a service-level protocol that lets customers lease a network's worth of computer power. Eucalyptus now works with Amazon's EC2 and may handle other client types with little tweaks and additions.

Nimbus
Nimbus is a free and open source cloud computing platform that offers infrastructure as a service. Users may rent distant resources and set up their own computing atmosphere by using virtual machines. All of these functional pieces may be broken down into three broad categories. Modules designed to work with clients are one kind and are used to support various cloud users. This category of part includes the context client module, cloud client module, reference client module, and EC2 client module. OpenNebula is the most common kind of second-level component. In addition to OpenStack, another open-source cloud service framework is OpenNebula . Users are able to install and operate virtual machines (VMs) on real resources, and their data centres or clusters may be transformed into a virtual infrastructure that can automatically adjust to fluctuations in service demand. OpenNebula lacks nimbus's implementation of a remote interface based on EC2 or WSRF via which users may manage all aspects of security. When used to coordinate storage, network, and virtual approaches, OpenNebula enables users to dynamically deploy services across the distributed infrastructure in accordance with allocation policies for data centre and distant cloud resources [9].

APPLICATIONS

Here are some examples of how cloud computing may be put to use

1) The cloud is a reliable and safe repository for storing information.
2) In addition, cloud computing enables cross-device data sharing.
3) In addition to number three, the cloud offers almost limitless potential for internet usage.
4) Users are not reliant on top-notch hardware to participate in cloud computing, and getting started is a breeze.
5) Companies and applications that rely on the underlying system infrastructure may become infrastructure- independent with the help of computing.
6) We can all reduce our outlay of initial capital and ongoing operating costs by making advantage of the Cloud's "pay as needed and on demand" infrastructure.

PROBLEMS WITH CLOUD COMPUTING.

As more and more personal and business data is stored on the cloud, questions regarding its security have arisen. The following is a summary of cloud computing problems

A. Privacy Users' private data may reside in several virtual data centres rather than in one central place, and users may unwittingly disclose non-public information when they use cloud computing services due to the underlying reliance on virtual computing. The crucial task may be analysed by attackers depending on the computing tasks that users provide.

B. Reliability Like our local server, the cloud servers sometimes go down or slow down.
Challenges from a Legal Perspective Concerns over security and personal privacy persist at all legislative levels.

D. Compliance Keeping up with the reporting and auditing needs imposed by the many laws that govern data storage and usage is a must. Data centres operated by cloud providers may potentially be subject to compliance standards in addition to the obligations to which clients are subject.

E. Freedom When using cloud computing, customers do not have access to the data on their own devices; instead, the cloud service provider acts as the data custodian and retains ultimate control over the data.

Perceptional Obstacles to Cloud Adoption
According to data gathered by IDC in 2008 from a survey
A. Security Data and software loss, phishing, and botnets (a network of computers controlled remotely) are all well-known security hazards to businesses. Shared resources (hard disc, data, VM) on the same physical system attract unforeseen side channels between a malicious resource and a normal resource due to the multi-tenancy concept and pooled computational resources in cloud computing. Furthermore, the problem of "reputation fate-sharing" will severely harm the reputation of many nice "citizens" of the Cloud who, unhappily, share the computing resources with a tenant who is known to be a malicious user. Due to the fact that they may share the same IP address, it will be impossible to tell the evil actors from the good ones.

B. Pricing Model When using the cloud, customers need to weigh the costs and benefits of computing, communication, and integration. Moving to the cloud may save money on expensive hardware, but it will cost more to send and receive data.

C. Rate Structure When compared to traditional data centres, which typically compute their costs based on consumptions of static computing, the cloud's elastic resource pool (through virtualization or multi-tenancy) has made cost analysis much more complex.

Level of Service Agreement (D) It is crucial for customers to get service level assurances from vendors. Service Level Agreements (SLAs) are contracts made between service providers and their customers to guarantee certain service levels.

CONCERNS ABOUT PRIVACY AND SECURITY

Due to its highly scalable nature, cloud computing can deliver an endless amount of computing resources on demand, meaning that cloud service providers don't have to make any long-term plans for hardware provisioning. Companies like Amazon, Google, Microsoft, and many more are racing to perfect cloud computing and expand the range of services it offers. In this study, we look at the issues of privacy and security surrounding existing cloud computing services offered by a variety of firms. The term "cloud computing" is used to describe both the services and the underlying infrastructures (i.e., the servers and operating systems) that make such services possible via the Internet. According to the research, customers find it difficult to adapt to cloud computing systems since the security and privacy guarantees offered by firms today are inadequate. So, it's important to think more about problems of security like availability, confidentiality, data integrity, control, audit, and so on. An On-Demand System for Safety Cloud services are software solutions delivered through a network, either privately or publicly, to a user. Without worrying about the qualities and locations of the underlying infrastructures, cloud computing enables providers to create, deploy, and execute applications with unlimited scalability (capacity), lightning-fast speed, and rock-solid dependability. The following five objectives may be met simultaneously by using cloud computing systems:

1) Availability When it comes to cloud computing, availability means making sure customers can access their data and apps whenever and wherever they choose. Since the cloud computing system is built from the ground up for the web, it offers customers a plethora of benefits. To be published in the December 2012 issue of the International Journal of Future Computer and Communication. 359 in order to use its components (e.g., programmes, services) from remote locations. All cloud-based computer systems have this property (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). The cloud computing system must always be available to all users so that they may access their data whenever they need to (say it is scalable for any number of users). The availability of cloud systems and the applications they host may be improved via the use of two key techniques: hardening and redundancy.

2) Confidentiality That entails ensuring the privacy of user information stored in the cloud. Cloud service providers have widely implemented two primary methods (i.e., physical isolation and encryption) to ensure data privacy.

Thirdly, the reliability of data Protecting data in the cloud (i.e., not lost or modified by unauthorised users). When it comes to offering services in the cloud, such as Data as a Service, Software as a Service, and Platform as a Service, ensuring data integrity is essential.

4) Controlling the cloud system entails controlling access to the system's resources, such as its applications, its infrastructure, and its data.

The fifth definition is "audit it," which entails monitoring activity in the cloud. Additional auditing capabilities might be included within the virtual machine's operating system (or application environment) housed on the hypervisor. The fact that it can monitor the full length of an access makes it far more secure than what is implemented in the apps or software.

CONCLUSION

In this article, we analysed the framework and prominent cloud computing platforms. It also provided in-depth solutions to cloud computing's problems and difficulties. Even with its many drawbacks and the need for improved procedures and processes, cloud computing is emerging as a very appealing paradigm, particularly for big businesses. Cloud computing efforts have the potential to drastically revolutionise IT and might have an impact on businesses within the next two to three years.

REFERENCES

1. Srivastava, P., & Khan, R. (2018). A review paper on cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(6), 17-20.
2. Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: implementation, management, and security*. CRC press.

3. Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421-426.
4. Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849-861.
5. Malik, M. I., Wani, S. H., & Rashid, A. (2018). CLOUD COMPUTING-TECHNOLOGIES. *International Journal of Advanced Research in Computer Science*, *9*(2).
6. Zhou, Y., Zhang, D., & Xiong, N. (2017). Post-cloud computing paradigms: a survey and comparison. *Tsinghua Science and Technology*, *22*(6), 714-732.
7. Namasudra, S. (2018). Cloud computing: A new era. *Journal of Fundamental and Applied Sciences*, *10*(2).
8. de Bruin, B., & Floridi, L. (2017). The ethics of cloud computing. *Science and engineering ethics*, *23*(1), 21-39.
9. Birje, M. N., Challagidad, P. S., Goudar, R. H., & Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. *International Journal of Cloud Computing*, *6*(1), 32-57.