IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 2, March 2022

A Review Paper on Cloud Computing

B. H. Rashmi, Bhoomika M., Puttaraj
Students, Department of Computer Science and Engineering
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *On demand or on pay per use of resource such as: network, storage and server these all facilities are provided by cloud computing through internet is called cloud computing. Although, cloud computing is facilitating the Information Technology industry, the research and development in this arena is yet to be satisfactory. We have contribution in this paper is an advanced survey focusing on cloud computing concept and most advanced research issues. This paper provides a better understanding of the cloud computing and identifies important research issues in this burgeoning area of computer science. Section 1 contains the introduction, in the section 2, we provide an overview of cloud computing, section 3 contains the security architecture and section 4 will focus on the research issues and security issue. We conclude the paper on section 5 along with references.*

Keywords: Cloud Computing; Security issue Virtualization; Data Center; Server Consolidation; cloud security.

I. Introduction

Cloud computing consists of three distinct types of computing services delivered remotely to clients via the internet. Clients typically pay a monthly annual service fee to providers, to gain access to systems that deliver software as a service, platforms as a service and infrastructure as a service to subscribers. Clients who subscribe to cloud computing services can reap a variety of benefits, depending on their particular business needs at a given point in time. The days of large capital investments in software and IT infrastructure are now a thing of the past for any enterprise that chooses to adopt the cloud computing model for procurement of IT services. The ability to access powerful IT resources on an incremental basis is leveling the playing field for small and medium sized organizations, providing them with the necessary tools and technology to compete in the global marketplace, without the previously requisite investment in on premise IT resources. Clients who subscribe to computing services delivered via the "cloud" are able to greatly reduce the IT.

II. Cloud Architecture

An Enterprise Cloud is a hosted computing environment that delivers software, platform or infrastructure services to business users via a network. Enterprise Cloud Computing provides organizations with the ability to deliver computing services in a controlled and secure manner, since a cloud for the enterprise makes use of a network firewall. Entities that store, mange or process sensitive data, including government agencies and health care organizations, are likely to use enterprise cloud computing services, as opposed to using public cloud computing services. Many businesses who own on-premise IT systems can maximize their IT investment through Enterprise Cloud Computing. A Cloud for the Enterprise promises to deliver an extremely agile computing environment for client users within private organizations. These organizations can gain many of the same **operational** benefits available within a public cloud computing environment. Extending a private cloud that incorporates methods such as virtualization, automation and service management; can result in increased operational efficiency within an organization.

2.1 Cloud Management Applications for IT Administrators

This combination of features allows fewer IT professionals to support a larger number of users and more hardware resources than would be possible under dedicated server/dedicated systems administrator approaches.

2.2 Identifying Weaknesses in Existing IT Service Delivery

IT departments have policies and procedures for delivery services. When new hardware is procured, there is a procedure to follow. When new applications are brought online, there are procedures to follow. The list could go on to include policies

DOI: 10.48175/IJARSCT-2856

and procedures that describe how to implement security controls, software maintenance, network management, and systems monitoring and auditing. Any one of these areas can represent a weakness in the ability to deliver IT services. Consider an example: A line of business wants to deploy a new service that will require several servers and a commonly used application stack. Everything the department wants is well within the ability of the IT department to support but still there are problems:

- The time required to review the server orders and verify the configurations are correct
- Determination of whether additional licenses are required to run the application stack
- Identification of IT staff to perform the installation and systems administration tasks
- Determination of where the hardware will be located and assurance that there is sufficient power, network connections, and other infrastructure to support the new servers

If this same new application were deployed in the cloud, we would still have to address these same issues, but we could do it more efficiently. Servers would not have to be ordered just for this application. A license management scheme (for example, site licenses) would presumably already be in place for cloud-based applications. The installation process would be reduced to ensuring the correct images are available in the service catalog. Application administrators would start virtual servers running the necessary applications on an as needed basis. Hardware would be in place, so questions about infrastructure would not arise. Implementation issues such as these put a drag on innovation or improvement to existing processes. By identifying steps in IT processes that hinder other business operations, we can better understand where we can apply cloud computing to avoid those issues.

2.3 Determining the Best Cloud Model for Your Requirements

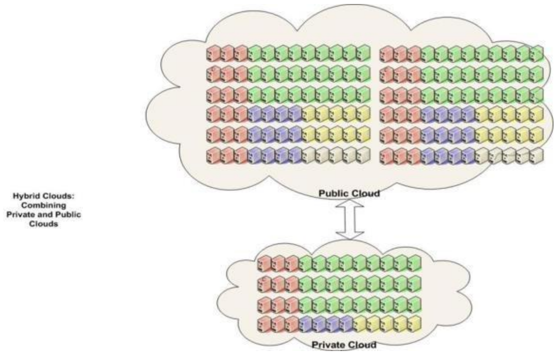
As we have described throughout this guide, there are three models for delivering cloud services: private, public, and hybrid. Which is the best option for you? A private cloud is suitable for enterprises that have the infrastructure, support skills, and management framework to maintain such an architecture. We use the term infrastructure broadly, to include not only IT hardware but physical infrastructure such as data centers, redundant power supplies, and multiple high-speed Internet connections. IT professionals running a private cloud will be required to manage large numbers of similarly configured servers, multiple disk arrays, a complex array of network management systems, and robust security controls. A management system must be in place as well to implement cost recovery, capacity planning, service delivery, licensing negotiations, and other administrative capabilities. These are significant barriers to adopting a private cloud model, but there are advantages as well. Your organization has complete control over the service catalog, who is allowed to use cloud resources, and the ability to monitor all cloud services. The fact that data and applications would not have to reside outside the corporate firewalls can be a substantial advantage from a compliance perspective.

A public cloud has several advantages:

- Minimal capital expenditures
- Ability to maintain existing infrastructure in its current configuration, allowing for a period of time in which both existing and new cloud-based instances are used
- Possibly lower costs per unit of computing service or storage because of the economies of scale
- Less management overhead for dayto-day operations but potentially more overhead for negotiating, monitoring, and enforcing SLAs

The potential drawbacks of a private cloud include the need to move sensitive data outside the corporate infrastructure, the potential costs of transmitting large volumes of data over the network, and the delays in moving data into the cloud by shipping storage devices (done in some cases to reduce upload costs). A hybrid cloud can offer the advantages of both the private and public cloud. Sensitive information can be maintained in a private cloud while other data is moved to the public cloud. Existing infrastructure can be readily redeployed to a cloud while older or less amenable hardware is not. Initial capital expenditures may be reduced because peak loads in the private cloud can be accommodated by allocating resources in a public cloud. Once again, there is no solution that is optimal for all cases. The advantages and disadvantages of each model must be weighed against the business requirements and constraints.

DOI: 10.48175/IJARSCT-2856



A combination of private and public clouds can enable an organization to realize the benefits of both.

2.4 Planning for Long-Term Management and Stability

Implementing a computing and storage cloud is a long-term proposition that requires attention to a number of areas in addition to those already mentioned. In particular, we need to plan for security, disaster recovery, and maintenance of physical infrastructure. Security considerations include protecting physical infrastructure as well as logical access to services and resources. Cloud data centers will require the same types of physical protections as one would find in any large data center. Access to infrastructure should be limited to those with legitimate needs. The site should be monitored and security procedures audited. Fire suppression equipment should be in place. Logical access controls begin with identity management. Policies should be in place defining who has access to various cloud resources, such as servers and applications. Licensing restrictions should be taken into consideration as well. Policies and procedures should define how authentication and authorizations are granted, monitored, and revoked. Longterm management includes planning for disaster. Maintaining multiple data centers may be a reasonable strategy for some private cloud users but not others. The costs can be prohibitive. One alternative is to use a public cloud for disaster recovery purposes, although there are still issues regarding confidentiality and compliance. Maintaining the physical infrastructure of a cloud is an ongoing operation. With large numbers of servers and disks, it is reasonable to expect regular equipment failures. Even with long mean times between failures, when we are dealing with thousands of pieces of equipment, parts will fail. Services, such as power and Internet access, will fail as well. Backup power supplies and redundant Internet providers should be used. A useful rule of thumb for managing cloud computing and the services it can provide is to assume that change and innovation are inherent. New equipment and applications will be added while others are retired. Equipment will fail. Power will go down. New business requirements will emerge. Cloud computing, like the business environment it serves, is dynamic.

2.5 Implementing a Cloud Infrastructure

Analyzing business drivers can be challenging because of complex, interdependent goals and objectives. Planning can be difficult because one has to merge both business requirements and technical constraints in a way that serves business objectives. The next stage of the process, implementation, is difficult primarily for technical reasons. The specific challenges will vary depending on the type of cloud model that is being used: private, public, or hybrid.

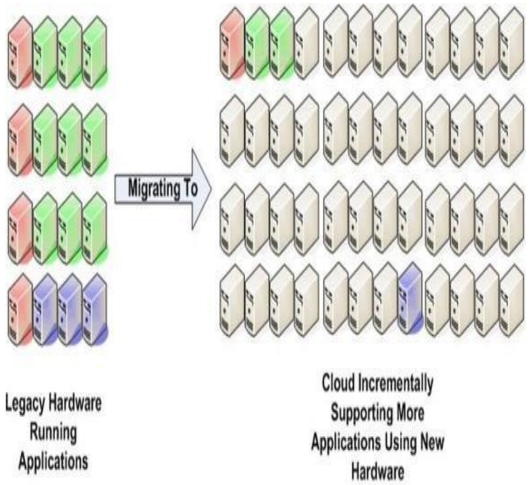
III. Implementing a Private Cloud

The key tasks to implementing a private cloud center on deploying hardware and establishing operations. Three such tasks are:

- Reallocating and deploying servers
- Establishing software and application management procedures
- Implementing a management framework

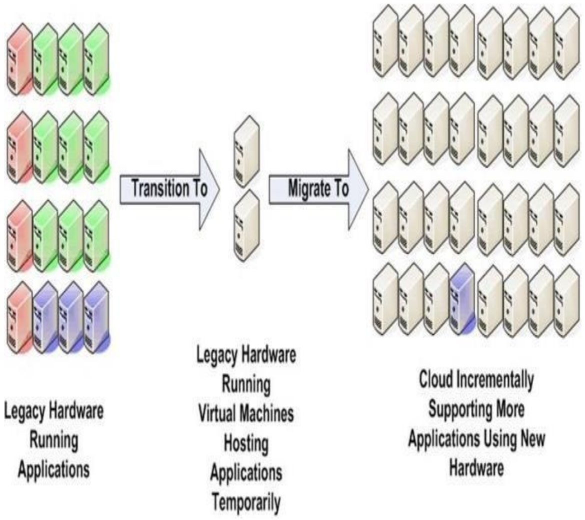
Reallocating servers must be done carefully to avoid disrupting existing business services. When new hardware is used for cloud deployments, the transition is relatively straightforward, as depicted. Applications can continue to run on legacy hardware as long as needed as those same applications are moved to the cloud.

DOI: 10.48175/IJARSCT-2856


Migrating To
Legacy Hardware Running Applications
Cloud Incrementally Supporting More Applications Using New Hardware

When new hardware is deployed in the cloud, applications can migrate directly to the cloud.

When existing hardware is redeployed to the cloud, the migration is less direct. A basic challenge is to keep services available while migrating hardware from an application centric use of servers to a cloud computing model. One way to handle this challenge is to migrate applications from their dedicated servers to a set of virtual machines running on servers temporarily allocated to support the migration. This approach works when servers dedicated to applications are not using the full capacity of servers. Applications are temporarily hosted on transition servers while hardware is migrated to the cloud. Once the hardware, software, and supporting cloud services are in place, applications can begin running in the cloud.


Transition To
Migrate To
Legacy Hardware Running Applications
Legacy Hardware Running Virtual Machines Hosting Applications Temporarily
Cloud Incrementally Supporting More Applications Using New Hardware

Applications may be hosted on transition virtual servers in cases where existing hardware is to be redeployed to the cloud.

Management procedures must be established for maintaining the diverse array of software that will be used in the cloud. These include establishing policies and procedures for:

- Adding and removing applications from the service catalog
- Patching images in the service catalog
- Controlling the use of licensed applications to ensure their use is in compliance with licenses
- Performing security reviews, such as vulnerability and malware scans on images in the service catalog

A private cloud also requires a management framework for non-software management issues. A number of essential management tasks should be in place before the cloud is widely used in the enterprise:

- Tracking compute and storage usage for billing and cost recovery purposes

DOI: 10.48175/IJARSCT-2856

- Monitoring performance and load for capacity planning
- Auditing patterns of use and access as part of security review procedures
- Introducing public cloud services brings with it a different set of implementation tasks.

IV. Adapting Public Cloud Services

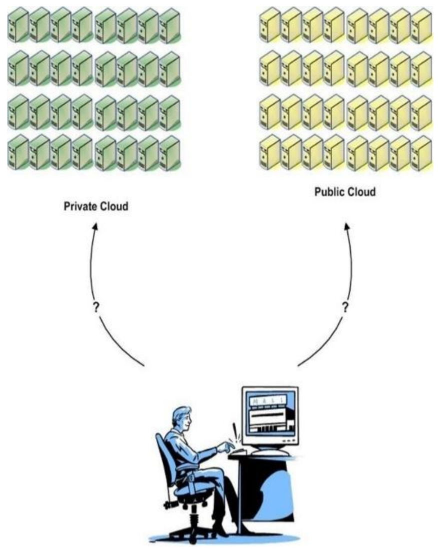
Using a public cloud relieves a business of many of the implementation tasks associated with private clouds. There is no need to transition hardware or redeploy servers. No service catalogs to establish and manage. No low-level billing infrastructure to put in place. Instead the focus tends to be more on defining SLAs and reviewing compliance and security issues. SLAs are essentially contracts between a business and a cloud provider. SLAs are important for clarifying what services are expected, the cost of such services, the quality of these services, and compensation for failure to meet agreements. SLAs with public cloud providers can include agreements about many factors:

- The number and types of servers that will be available for use at any time
- Restrictions on the number of virtual or dedicated servers that may be allocated in a single request
- Minimum and maximum storage usage
- Guaranteed bandwidth into and out of data centers used by the public cloud
- Security controls and procedures
- Audit and monitoring responsibilities of the provider and the business customer
- Compute and storage rates, billing periods, and so on
- Individual and aggregate demand reports

Several of the topics addressed in SLAs are security oriented. Clearly, a top priority for most businesses using public cloud services is ensuring that private, sensitivity, and confidential data is protected. This will require a combination of secure communications between the cloud data center and user sites; secure, probably encrypted persistent data storage in the cloud; access controls on private images or applications stored and run in the cloud; and verification that cloud software is routinely patched and scanned for vulnerabilities and malware.

V. Using a Hybrid Private-Public Cloud

A hybrid private-public cloud delivers the benefits of both models of cloud computing. It also brings with it the responsibilities of both that we just described—and a bit more. The combined resources of a private and public cloud may appear to be seamlessly integrated from the users' perspective but there are operational differences. Only data and applications that are deemed safe to store or run in a public cloud should be made available outside the private cloud.



If users are given a choice of where to run applications in a hybrid cloud, policies and incentives should be in place to promote the optimal balance from an enterprise perspective**.** Users of cloud services should also be made aware of any cost differences between the private and public clouds. For example, will the IT department charge an additional fee on top of the public cloud provider's charges to cover the overhead of managing the hybrid cloud? Also consider whether rules or cost structures should be in place to incentivize users to use private cloud services before turning to the public cloud. This is especially important if cost recovery pricing is used and assumptions are made about the level of utilization in the private cloud. The last key area to address for the long-term maintenance of an enterprise cloud is, in fact, maintenance.

VI. Managing and Maintaining a Cloud

The tasks of managing and maintaining a cloud computing environment can be broken down into operational issues and business management issues.

6.1 Cloud Computing Security Issues

Security is very crucial factor. First thing that people think is to avoid the private data in cloud. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Security Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft. Privacy Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users. Reliability Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk. Legal Issues Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones". On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels. Open Standard IJSER International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2124 ISSN 2229-5518 IJSER © 2013 http://www.ijser.org Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices. Compliance Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements. Freedom Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring. Long-term Viability You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

VII. Conclusion

In this paper we discuss about the emerging technology and its architecture including various Layers. Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. In this paper the benefits and security issues are addressed as well. There are some security measures and some are under research that Provide Security on each layer that we discuss in this paper. Security in cloud computing consist of security abilities of web browsers and web service structure. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection. The deployment models are also discussed that help in retrieving the information. SAAS, PAAS, IAAS are the three models for cloud computing. It opens up the world of computing to a broader range of uses and increases the ease of use by giving access through any internet connection. However, with this increased ease also come drawbacks. You have less control over who has access to your information and little to no knowledge of where it is stored. You also must be aware of the security risks of having data stored on the cloud. There are various technological perspectives for cloud analytics and various cloud services that can be envisaged in future, as the development of cloud computing technology is still at an early stage

References

[1]. Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0 – March

[2]. Ross A. Lumley, " Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business" Report GW-CSPRI-2010-4 December 18, 2010

[3]. Amoretti, M., Laghi, M. C., Tassoni,F., Zanichelli, F.: Service Migration within the Cloud: Code Mobility in SP2A. Proceedings of International Conference on High Performance Computing and Simulation (HPCS),2010, pp.196-202.

[4]. Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

[5]. Gerald Briscoe and Alexandros Marinos. "Digital Ecosystems in the Clouds: Towards Community Cloud Computing,"2009, http://arxiv.org/pdf/0903.0694v3.

[6]. Peter Mell and Tim Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Information Technology Laboratory. Version15,2009. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-defv15.doc

[7]. Fallenbeck, N., Picht, H.J., Smith, M. and Freisleben, B.: Xen and the Art of Cluster Scheduling. In Washington: 2nd IEEE International Workshop on Virtualization Technology in Distributed Computing (VTDC '06).

[8]. Zhang, H., Jiang, G., Yoshihira, K., Chen, H., Saxena, A.: Intelligent Workload Factoring for a Hybrid Cloud Computing Model. In California : International Workshop on Cloud Services, Los Angeles, July, 2009.

[9]. Armbrust M et al (2009) "Above the clouds: a Berkeley view of cloud computing". UC Berkeley Technical Report

DOI: 10.48175/IJARSCT-2856