Journal of Innovative Engineering and Research (JIER)
Vol.- 3,Issue - 2,October 2020, pp. 16-19 (4 pages)

An Analysis of Multi-Cloud Environment with Security Challenges

RAVI PATHARIA, Dr. SANJAY SINGH BHADORIYA

Department of Computer Application, Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: akshpatharia@gmail.com

Abstract— Cloud computing is a service of delivering IT resources as a service through the Internet. Cloud computing has become increasingly important in terms of data storage and lowering overall costs for organizers. Cloud computing security is a critical element of the cloud computing environment. Users frequently save sensitive data on cloud storage services, however, these companies may be untrusted. Recently, there has been a trend toward "multi-clouds," also known as "cloud-of-clouds ". In this paper, we will discuss about cloud model, services, and the security limits of a single cloud, as well as the benefits of implementing a multi-cloud approach.

Index Terms— Cloud computing, Cloud services, Single cloud, Multi-cloud, Security.

I. INTRODUCTION

Data The cloud is a growing technology in the computer field. It refers to the accessing of information and software applications through the internet. The Software as a service (SAAS), Platform as a service (PAAS), and Infrastructure as a service (IAAS) services are provided by cloud computing. The services are hosted at the data centre by the cloud service providers for the organization or the individual users to utilize the services through a network connection. Companies that offer various cloud services are referred to as cloud service providers. Cloud computing is associated with growing technology, high-cost data storage devices, and a quick rate for various cloud services, including Infrastructure as a Service, Software as a Service, and Platform as a Service. The cloud storage moves the customer data to large data centres which are remotely located. There are lots of data Security issues in Single Cloud. Multi-cloud services provide solutions to data security and data storage problems. Multi-cloud is more than one cloud computing service from any number of different vendors of the cloud. A multi-cloud environment could be a combination of all-public, all-private, or both.
The study of single cloud services and multi-cloud computing environments, as well as effective resource sharing among cloud services, is proposed in this work.

II. CLOUD COMPUTING SERVICE MODEL

Three different services are grouped as:
Software as a service, Platform as a service and Infrastructure as a service each with unique features.
Software as a service (SaaS). "On-demand software" is another term for SaaS. It's a type of software where the applications are hosted by a third-party cloud service provider. Users can use a web browser and an internet connection to access these applications. Google Apps [1]
Platform as a service (PaaS) provides a platform for building and running custom applications. PaaS is allowing the customer to rent virtualized servers and attached services to execute available applications or develop and test the new one [2].The Google App Engine and Microsoft Azure [1] are examples of the PaaS.
Infrastructure as a service (IaaS) this infrastructure delivered as a service includes hardware (servers, networks, load balancers, etc). IaaS model is a result of the evolution of virtual private servers which has been already known many years back [3].Examples of IaaS providers are Amazon, GoGrid, 3tera, etc [4]

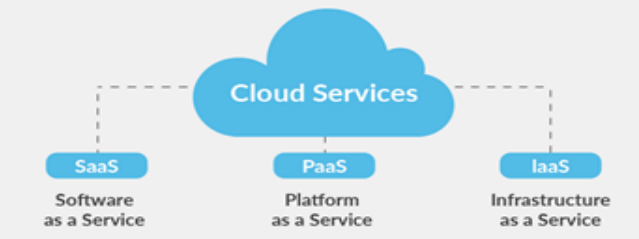

Figure 1: Cloud Service Model

III. TYPES OF CLOUD COMPUTING

There are public and private clouds that offer complementary benefits, there are three basic service models to consider, and there is the value of open APIs versus proprietary ones [5].
Public Cloud: In the public cloud, the computing infrastructure is hosted by the service provider. The services offered by third-party providers through the public Internet.The client has no control over and visibility where the computing infrastructure is hosted. Examples of public cloud are Google, Gmail, Google Drive, Amazon, and Microsoft.

Figure 2: Public Cloud

Private Clouds: Private clouds are designed for a single client's exclusive usage, giving them maximum control over data, security, and service quality. The infrastructure is owned by the firm, and it has complete control over how applications are placed on it. Microsoft Azure Stack, Ubuntu, and HP Data Centres are private cloud companies. This model gives companies a high level of control over the use of cloud resources while bringing in the expertise needed to establish and operate the environment. [6].

Figure 3: Private Clouds

Hybrid cloud: It is cloud computing that combines one or more public clouds with a private cloud service, a hybrid cloud also can be used to handle planned workload spikes. Hulu, Netflix, Uber, and Airbnb.

Figure 4: Hybrid cloud

Community Cloud: A hybrid form of private cloud is Community Cloud. Community Cloud is a distributed infrastructure service provided by different types of cloud solutions that solves the specific issues of business sectors by accommodated.

The main purpose of all these services is to allow different customers to collaborate on community-related applications and projects that require a centralized cloud infrastructure.

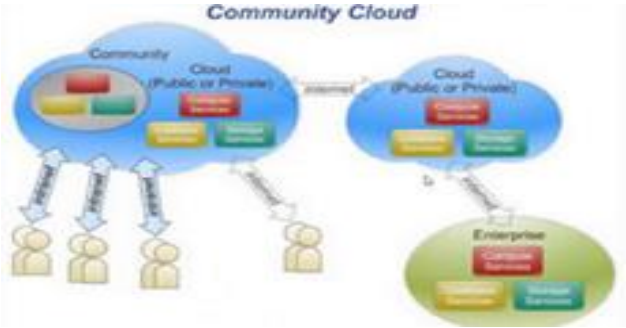

Figure 5: Community cloud

IV. EMERGING ISSUES AND MOTIVATION OF CLOUD COMPUTING

1. Cloud computing technology has become a slogan in today's digital world and generates thousands of terabytes of digital data every day. By building a private cloud in the company, this data can be stored securely. These private clouds are limited by flexibility and scalability due to their limited capacity and therefore have their limitations [7]. These organizations do not want to migrate to a public cloud that will overcome all these limitations due to business continuity threats or vendor locks.

2. Hybrid cloud potentially combines the benefits of private and public (external) clouds. By efficiently using the features of multiple external clouds and storing data by selecting multiple clouds for storage, vendor locking can be avoided. Traditionally, most companies have their own IT department (IT) that supports daily business transactions and processes. For small and medium-sized businesses, having IT infrastructure is very expensive because they not only have to invest heavily in IT hardware and software but also in IT staff, maintenance, and daily operating costs. With the advent of the Cloud, most organizations are now migrating outsourcing IT requirements to achieve cost-saving benefits. During this period, many organizations opted for cloud services. This allows customers to choose from a range of service providers at a competitive price. In the current ten years, although researchers have proposed many frameworks to solve these problems, the research work is mainly focused on the work related to the security of data stored in the cloud, but the work done to solve the security problem, is limited.

3. Data storage on the Multi-Cloud platform using file storage. File storage is considered one of the enterprise solutions to meet storage needs. For companies, it is very important to ensure data security before data is stored in the public cloud. In today's IT environment, requirements for price, performance, uptime, and availability have led to a number of storage requirements. In file storage, the file system is used to access space. Many researchers have developed a security model for object storage, which is more suitable for storing and retrieving individual data. Most importantly, object storage is not suitable for partial recall and updating of data objects.

4. Most of the frameworks proposed by various researchers for storage in a multi-cloud environment (such as MCDB, Hail, RACS, Cloud-Raid, Depsky-A, Depsky-CA, NC-Cloud, and Triones) are committed to confidentiality, integrity Increased sexuality or applicability. Or solve problems with supplier locking or optimal storage. All these methods only solve the object storage technology.

5. Multi-cloud implementation is one of the areas that cloud technology researchers have recently focused on. However, due to the growing popularity of cloud computing, cloud service providers (CSPs) have provided a range of options that provide a wide range of QoS (cost and service of quality) products, allowing the choice of cloud providers to build Multi-Cloud faces challenges.

6. The features of cloud IT configuration models (such as multi-tenancy, virtualization, and resource sharing) add some difficulties with billing estimation during the application design and deployment phase. This is one of the main reasons

why consumers avoid migrating to the cloud or multi-cloud. However, there are other reasons for the need for a multi-cloud framework, especially in the storage-as-a-service model, such as vendor locking, availability, confidentiality, and security.

7. Federated cloud and multi-cloud are two delivery models for multiple clouds, and both differ in terms of the agreements between the various cloud providers involved. In the case of a federated cloud, there are reciprocal agreements between different cloud providers, while multi-cloud clouds do not require agreements. Since there is no need to sign an agreement before a multi-cloud is formed, multiple cloud provider options can be used, increasing the complexity of maintaining a single service level agreement (SLA). Master SLA generation reduces the complexity of tracking SLAs. For multi-cloud solutions, most of them have not yet discussed the impact of a single CSP service level agreement on multi-cloud solutions. In addition, there are few SLA generation methods for multi-cloud solutions, but most methods do not discuss its impact on SLA attribute implementation technology.

8. In the "storage-as-a-service multi-cloud" scenario, it is necessary to introduce SLAs in two layers, one layer is used to guide SLAs from different cloud providers that are part of "storage-as-a-service multi-cloud ", and the second layer is used to manage the largest SLA for users. The multi-cloud implementation using erase coding technology distributes user data in different cloud infrastructures with different QoS attributes. From the user's perspective, it can be seen as a composite infrastructure service with a set of functional and non-functional requirements for storing user data.

9. Due to the diversity of cloud provider services, it is a difficult task to select cloud providers based on user needs, expert ratings, and past performance of service providers and to select appropriate services to form a multi-cloud. In addition, the QoS parameters mentioned in user requirements may have conflicts or different degrees of significance between different cloud providers or when using different methods to calculate attributes. Due to the diversity of cloud provider services, it is a difficult task to form a multi-cloud environment to choose a cloud provider based on the above three parameters.

10. Makris et al. Proposed the use of different multi-criterion decision-making methods (MCDM) in web services and cloud computing based on SLA QoS service selection research work, but the application of the MCDM method in cloud computing research work is limited to choosing a single service based on ranking Provider or more attribute decision methods. Due to multi-tenancy and outsourcing, ie data on a multi-cloud, it is necessary to ensure data integrity through public verifiability and availability in the storage-as-a-service model of a multi-cloud as a service environment. Data stored in private or public clouds are not controlled by users and are managed and shared by insecure and untrusted servers [8], [9].

11. To ensure the accuracy of the data, Lamb et al. The task of allowing a third-party auditor (TPA) on behalf of the cloud client to use different techniques to verify the integrity of the data stored in the cloud has been considered. Chervenak et al. proposed a system for secure access and identity verification for cloud service providers [10].

In addition, the confidentiality of outsourced data needs to be improved. The task of hiding information can be accomplished using encryption algorithms. Since all encryption algorithms require the parties to exchange keys, it has its concern that the key will be lost to a third party. Therefore, problems related to key distribution must also be addressed. In light of the above statement, the challenge is to deliver all security features cost-effectively. Therefore, the entire cloud community relies on a set of algorithms that can process and protect data without consuming a lot of resources. Since the network uses many algorithms to protect its data, the user's first task is to analyze the set of algorithms used.

V. LIMITATION OF SINGLE CLOUD

There are multiple problems in the single cloud one of the security issues. The Complete data may be lost or damaged during transmission between client and cloud provider. Its security should be taken into consideration as Data Integrity. Data confidentiality and protection of sensitive data, such as bank account detail or confidential data, should be protected. In a single Cloud provider, there is no backup solution so data availability more difficult.

VI. REASONS FOR MULTI-CLOUDS

The multi-cloud approach is a cloud storage architecture that builds a virtual cloud storage system by using a combination of different cloud storage services. The data to be stored is divided into several blocks and distributed on different cloud storage providers redundantly. Since sensitive data should not be transferred to a single cloud to avoid relying on just one cloud provider, there is a great need for multiple clouds. Therefore, cloud computing needs to be switched from a single cloud to a multi-cloud to achieve data security.

Improve privacy, public verifiability, and authorized access to data in multiple clouds. : When you access data, data may be compromised or lost due to hardware failure. Therefore, data must be verified and accessed by authorized users. The following are the factors of Cloud Security.

- Confidentiality
- Privacy
- Integrity
- Availability

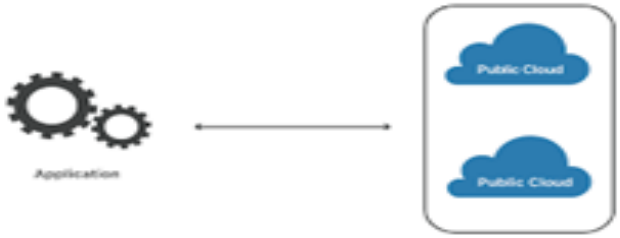

Figure 6: Multi-cloud

VII. EXISTING MULTIPLE-CLOUDS TYPES

Intra Cloud: This cloud has two or more different services that belong to the same cloud provider and that collaborate.

Hybrid cloud: This is a combination of a private and single cloud, and is used when the private cloud cannot deal with the processing and /or data load.

Federated Clouds: It has two or more independent cloud service providers that agree to share their infrastructure and work together to share resources and provide the necessary services with agreed service quality.

Multi-cloud: It is more than an independent cloud that will be used to perform requested tasks through available resources. The customer is responsible for resource/function management, task planning, and load balancing.

VIII. CONCLUSION

For In this paper different features and problems are discussed about single cloud computing also discussed the environment of multi-cloud computing. Multi-cloud can solve all data storage-related security issues and resolve data availability and vendor lock issues to overcome storage access, mobility, cost, privacy, vendor lock issues, cross-virtual machine issues, etc. (VM) attacks, interoperability, efficiency, generation, and monitoring, etc. Therefore, it is necessary to develop a framework that addresses all of the above shortcomings of existing systems. Also require a design of secure resource sharing, interconnectivity multi-cloud environment with migrating applications to a targeted cloud computing model or models is a demanding task.

REFERENCES

1. Lin and Shih " Cloud computing: The Emerging Computing technology", July 2010
2. S. Khurana and A. G. Verma, "Comparison of Cloud Computing Service Models: SaaS ,PaaS , IaaS," Int. J. Electron. Commun. Technol., vol. 7109, pp. 29–32, 2013
3. C. N. Höfer and G. Karagiannis, "Cloud computing services: Taxonomy and comparison," J. Internet Serv. Appl., vol. 2, no. 2, pp. 81–94, 2011.
4. M. Rajendra Prasad, R. Lakshman Naik**, V.Bapuji "Cloud Computing: Research Issues and Implications "International Journal of Cloud Computing and Services Science, Vol.2, No.2, April 2013, pp. 134~140 ISSN: 2089-3337
5. Sun Microsystems ,"Introduction to Cloud Computing Architecture" White Paper 1st Edition, June 2009, pp. 01-35
6. Ramachandran S, "Cloud Computing: The Next Generation of the Internet" IJCST Vol. 3, Issue 1, pp. 396 -399, Jan. - March 2012,
7. Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng and Jiunn-Chin Wang, ―A Study of CAPTCHA and its Application to user Authentication‖, Proceeding of 2nd International Conference on Computational Collective Intelligence: Technologies and Applications, 2010
8. X. Wang, X. Wang, K. Zheng, Y. Yao, and Q. Cao, "Correlationaware traffic consolidation for power optimization of data center networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 992–1006, April 2016.
9. J. Son, A. V. Dastjerdi, R. N. Calheiros, and R. Buyya, "SLA-aware and energy-efficient dynamic overbooking in SDN-based cloud data centers," IEEE Transactions on Sustainable Computing, vol. 2, no. 2, pp. 76–89, April 2017.
10. M. Al-Fares, A. Loukissas, and A. Vahdat, "A scalable, commodity data center network architecture," in Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication. New York, NY, USA: ACM, 2008, pp. 63–74.