International Journal of Research in Engineering, Science and Management
Volume-2, Issue-9, September-2019
www.ijresm.com | ISSN (Online): 2581-5792

Creation of Virtual World with the Evolution of Cloud Computing

Amritaticku[1], Deepika Yadav[2], Amit Sharma[3]
[1,2]*AssistantProfessor, Department of Computer Science and Engineering, B. S. Anangpuria Institute of Technology and Management, Faridabad, India*
[3]*Senior Software Engineer, ATMECS Technologies Pvt. Ltd, Hyderabad, India*

***Abstract*: Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.**

Cloud computing is usually described in one of two ways. Either based on the deployment model, or on the service that the cloud is offering.

Based on a deployment model, we can classify cloud as: public, private, hybrid and community cloud.

***Keywords*: virtual world, cloud computing**

1. Introduction

Based on a service the cloud model is offering, we are speaking of either:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- or, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service

Basically, programs that are needed to run a certain application are now more popularly located on a remote machine, owned by another company. This is done in order not to lose on the quality performance due to processing power of your own computer, to save money on IT support, and yet remain advantageous on the market. These computers that run the applications, store the data, and use a server system, are basically what we call "the cloud".

A. Working of different types of cloud

Public Cloud:

When we talk about public cloud, we mean that the whole computing infrastructure is located on the premises of a cloud computing company that offers the cloud service. The location remains, thus, separate from the customer and he has no physical control over the infrastructure.

As public clouds use shared resources, they do excel mostly in performance, but are also most vulnerable to various attacks.

Private Cloud:

Private Cloud provides the same benefits of Public Cloud, but uses dedicated, private hardware. Private cloud means using a cloud infrastructure (network) solely by one customer /organization. It is not shared with others, yet it is remotely located. The companies have an option of choosing an on premise private cloud as well, which is more expensive, but they do have a physical control over the infrastructure.

The security and control level is highest while using a private network. Yet, the cost reduction can be minimal, if the company needs to invest in an on premise cloud infrastructure.

Private Cloud provides following services:

- Increased redundancy
- Decreased provisioning time for new servers
- Saved capital by eliminating hardware support contracts
- Quicker expendability compared to hosting your own physical servers
- Use of dedicated, private hardware

Hybrid Cloud:

Hybrid cloud, of course, means, using both private and public clouds, depending on their purpose. For example, public cloud can be used to interact with customers, while keeping their data secured through a private cloud. Most people associate traditional public cloud service with elastic scalability and the ability to handle constant shifts in demand. However, performance issues can arise for certain data-intensive or high-availability workloads.

Some companies offer combines hybrid cloud with bare-metal and virtualized clouds into a unified environment allowing business to optimize for scale, performance and cost simultaneously.

Community cloud:

It implies an infrastructure that is shared between organizations, usually with the shared data and data management concerns. For example, a community cloud can belong to a government of a single country. Community clouds can be located both on and off the premises.

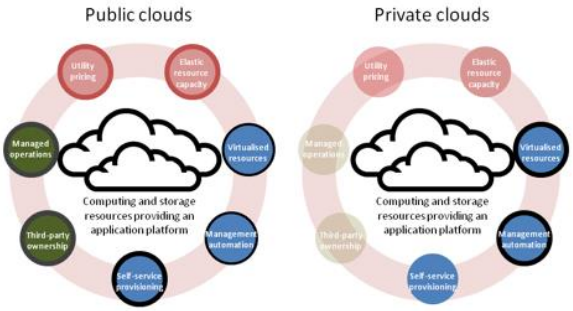

Fig. 1. Private vs. Public Cloud
(Image Source: Talk Cloud Computing)

Cloud Service Applications:

The most popular services of the cloud are that of infrastructure, platform, software, or storage. The most common cloud service is that one offering data storage disks and virtual servers, i.e. infrastructure.

Examples of Infrastructure-as-a-Service (IaaS) companies are Amazon, Rackspace, and Flexi scale. If the cloud offers a development platform, and this includes operating system.

If the cloud offers a development platform, and this includes operating system, programming language execution environment, database, and web server, the model is known as Platform-as-a-Service (PaaS)

Examples of which are Google App Engine, Microsoft Azure, Salesforce. Operating system can be frequently upgraded and developed with PaaS, services can be obtained from diverse sources, and programming can be worked in teams (geographically distributed).

Software-as-a-Service (SaaS), finally, means that users can access various software applications on a pay-per-use basis. As opposed to buying licensed programs, often very expensive. Examples of such services include widely used GMail, or Google Docs.

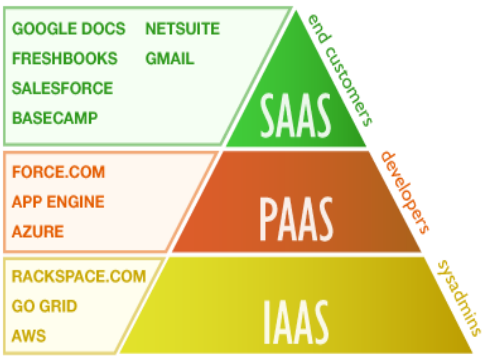

Fig. 2. Cloud Services Types and Examples
(Image Source: The Gadget Square)

The longer list will include

- Storage as a service (STaaS),
- Security as a service (SECaaS),
- Data as a service (DaaS),
- Test environment as a service (TEaaS),
- Desktop as a service(DaaS),
- API as a service (APIaaS).

Once you have understood the types of cloud computing, based on location and services, the most important step is to choose the right type of cloud and service, for a specific task with your clients.

Managing cloud infrastructures can be substantially more complex than traditional data infrastructures; however, cloud infrastructures have the potential to become highly optimized, intelligent systems that improve enterprises. Succeeding on the cloud means making the right business decisions and executing the right technological choices. At scale, these challenges get incredibly complex.

There are many companies that provide some of the most advanced technologies and solutions to help in reducing costs, manage cloud infrastructure and increase security of your public or hybrid clouds.

Cloud Management Platform:

Moving the business infrastructure to the cloud offers many benefits, compared to having to rely on the traditional, on-premises infrastructure. Efficiency, scalability, security and cost reduction are some of the major benefits that cloud offers organizations. Still, companies who use the cloud often see their expenses rise over time. This happens because, as business expands, it gets harder and harder for companies to monitor all processes and resources related to cloud-based operations.

Managing cloud infrastructure becomes a set of tasks that require extra time and financial resources. It can be substantially more complex than traditional data infrastructures due to the huge amounts of constantly changing data.

For large enterprises that rely on business data to outperform competition, the only viable approach to analyze the data and optimize their cloud resources is by using data science and machine learning.

Third Party Companies helps you quantify, understand, optimize, and automate your infrastructure, to control your data through knowledge.

Management Platform through which you can monitor and optimize your cloud processes and resources to the smallest detail.

Challenges in Cloud Environment:

Large enterprises usually have many DevOps teams working on several projects simultaneously, in different cloud environments. The problem with this setup is that it causes friction and slows down development. Here we need to enable self-service & direct AWS, Azure and GCP access for all your applications and developers.

Developing applications collaboratively creates unique challenges for security teams. Business partners faced with weeks or months of project delays often resort to starting application development offsite with their vendor to “accelerate” the project. Late in the project they discover that key enterprise controls were not considered part of the requirements, causing delays and rework.

We have to address the most common cloud challenges faced by large enterprises:

- Lack of resources/expertise
- Security
- Managing cloud spend
- Compliance
- Governance/control

Cloud Optimized Routing:

If you're a SaaS provider, you know that sub-second application response time is an important but often unrealized goal.

Research has consistently shown that an application response time of over 1 second will cause an interruption in the user's flow of thought, and a delay of about 10 seconds will result in the abandonment of the task.

The problem with slow application response time usually come from the Internet Backbone problem. The Internet Backbone is made up of many large Network Service Providers that interconnect with each other. These large networks charge Internet Service Providers (ISPs) to transport data packets long distances.

Within the Internet Backbone, all traffic is treated equally, and so ISPs maximize profitability by minimizing the cost of sending traffic. Least cost routing is the process of selecting the path traffic will take along the Internet Backbone based on the lowest cost, not on best performance. To solve this an Internet Overlay Network is required. Internet Overlay Network leverages the surface area of public cloud providers to continuously monitor the global Internet Backbone to find the fastest routes, avoiding congestion and overcoming the performance problems caused by least cost routing. In the process, it can improve data transfer performance by 10x or more.

Benefits you get from this solution:

- Fast, seamless content collaboration
- Dynamic SaaS performance
- Expansion to new geographies
- Secure private network

Cloud Security:

Cloud computing continues to transform the way organizations use, store, and share data, applications, and workloads. It has also introduced a host of new security threats and challenges. With so much data going into the cloud—and into public cloud services in particular—these resources become natural targets for bad actors.

One of the biggest concerns business owners, CTOs and everyone involved with IT decisions in a company have, is related to the security of the cloud infrastructure.

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Concerns associated with cloud computing security fall into two broad categories:

- Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud)
- Security issues faced by their customers (companies or organizations who host applications or store data on the cloud)

Cloud Web Application Firewall (WAF) stops OWASP security threats the moment they happen. It makes sure that data is protected from all threats non-stop, working together to stop all possible cyberattacks the moment they happen.

DDoS Protection and Mitigation for Cloud Applications

Every day nearly 3000 websites become victims of a DDoS attack. And while many sites are back up and running within hours, the damage to both revenue and customer trust can devastate a business for years.

A distributed denial-of-service (DDoS) attack is a cyber-attack in which an attacker renders a website unavailable to users by attacking it with multiple compromised systems (botnet).

All organizations suffer from DDoS attacks at some point in time, so it's crucial to have a cloud protection stack in place. Network DDoS attacks, such as SYN Flood and DNS Amplification attacks, are quickly growing in size. This is why the appropriate capacity for mitigation needs to be provided.

Through partnering with different service providers, we can offer robust CDNs that leverages a global network of strategically positioned servers to provide you the capacity to mitigate even multi-gigabit DDoS attacks.

Our platform provides automated DDoS attack protection at the network layers. These types of attacks are often referred to as Layer 3/4 attacks (aka volumetric attacks) since they effect the lower layers of the OSI Model (Network and Transport). Some examples of types of attacks include:

- SYN Floods (Spoofed IPs, non-standard TCP flags),
- UDP Floods,
- IPSec flood (IKE/ISAMP assoc. attempts), IP/ICMP fragmentation,
- NTP / DNS / SSDP reflection,
- SMURF,
- DNS flood

These attacks are generally designed to overwhelm the servers, ultimately resulting in a denial of service for legitimate traffic and disrupting the operation of the network.

Cloud Web Application Firewall (WAF) stops OWASP security threats the moment they happen. It makes sure that data is protected from all threats non-stop, working together to stop all possible cyberattacks the moment they happen.

DDoS Protection and Mitigation for Cloud Applications:

Every day nearly 3000 websites become victims of a DDoS attack. And while many sites are back up and running within hours, the damage to both revenue and customer trust can devastate a business for years.

A distributed denial-of-service (DDoS) attack is a cyber-attack in which an attacker renders a website unavailable to

users by attacking it with multiple compromised systems (botnet).

All organizations suffer from DDoS attacks at some point in time, so it's crucial to have a cloud protection stack in place. Network DDoS attacks, such as SYN Flood and DNS Amplification attacks, are quickly growing in size. This is why the appropriate capacity for mitigation needs to be provided.

Through partnering with different service providers, we can offer robust CDNs that leverages a global network of strategically positioned servers to provide you the capacity to mitigate even multi-gigabit DDoS attacks.

Our platform provides automated DDoS attack protection at the network layers. These types of attacks are often referred to as Layer 3/4 attacks (aka volumetric attacks) since they effect the lower layers of the OSI Model (Network and Transport). Some examples of types of attacks include:

- SYN Floods (Spoofed IPs, non-standard TCP flags),
- UDP Floods,
- IPSec flood (IKE/ISAMP assoc. attempts), IP/ICMP fragmentation,
- NTP / DNS / SSDP reflection,
- SMURF,
- DNS flood

These attacks are generally designed to overwhelm the servers, ultimately resulting in a denial of service for legitimate traffic and disrupting the operation of the network.

Cloud Security as a Unified Service:

To simply the process of managing different cloud infrastructures, international office branches and data centers, which delivers a cloud-based SD-WAN with built-in network security stack for all enterprise locations, cloud resources and mobile users.

It may offers a complete solution for modern enterprise's cloud needs: from a global, SLA-backed backbone, DDoS and Bot Protection to integration of multiple cloud environments into a single network.

2. Conclusion

Cloud computing is a virtual environment that can adapt to meet user needs. It is not constrained by physical limits, and is easily scalable – making it an obvious choice for start-ups. Cloud computing makes state-of-the-art capability available to anyone with an internet connection and a browser, reducing hardware and IT personnel costs.

References

[1] Bhushan Lal Sahu, and Rajesh Tiwari, "A Comprehensive Study on Cloud Computing," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 9, September 2012.

[2] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843-859, Second Quarter 2013.

[3] V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment," in *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, pp. 60-75, March 2014.

[4] Mladen A. Vouk, "Cloud Computing Issues, Research and Implementations", *Journal of Computing and Information Technology*- CIT 16, vol. 4, pp. 235–246, 2008.

[5] R. Moreno-Vozmediano, R. S. Montero and I. M. Llorente, "Key Challenges in Cloud Computing: Enabling the Future Internet of Services," in *IEEE Internet Computing*, vol. 17, no. 4, pp. 18-25, July-Aug. 2013.

[6] I. Bojanova, J. Zhang and J. Voas, "Cloud Computing," in *IT Professional*, vol. 15, no. 2, pp. 12-14, March-April 2013.

[7] SATW, "White Paper Cloud Computing".

[8] Harjit Singh, "Current Trends in Cloud Computing-A Survey of Cloud Computing Systems," in *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 3, pp. 1214-1219.

[9] Conway, Gerard and Curry, Edward, "Managing Cloud Computing: A Life Cycle Approach," *CLOSER 2012 - Proceedings of the 2nd International Conference on Cloud Computing and Services Science*, 2012.