International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Cloud Computing Using Cloud-Level Scheduling: A Survey

Sanket Mani Tiwari

Department of CSE, Galgotias University, Uttar Pradesh, India

Abstract: ***In recent years cloud computing are widely used everywhere. Cloud computing have wide variety of facility in his environment. Cloud provides many facilities due to its wide area such that sharing of resources for different purposes scheduling become a necessary factor to discuss. A numerous type of applications are running through cloud which are stored in data centers. Data centers are combination of place which acts like database. For example applications like we chat are running using cloud. All data is stored in data centers and user just retrieve information from these data centers which is required and other information is available for other users an high security is also possible for end user using cloud. Cloud based on virtual machine concept, this machine run on physical machine. Virtual machine incorporate the optimized hardware resources called virtualization, this virtual machine creates large data centers used commonly that based on virtual machine called clouds. Cloud computing carry both high-availability storage of data as well as high parallel computing resources. Cloud computing based on the concept of scheduling that carry many job in a particular manner, job scheduling is very tedious task in cloud computing. Because it is carry the concept of parallel and distributed architecture. In recent year's computer service is a fast approach because of parallel computing, distributed computing, grid computing and cloud computing. In this survey we conclude the cloud level scheduling having trust based security and we also prefer the reliability factor that calculate the estimated cost as well as migrate the scheduling process.***

Keywords: Cloud security, Data storage, Service delivery model, IaaS, PaaS, SaaS, Scheduling, Cloud level scheduling.

1. Introduction

Cloud computing is known as a provider of dynamic services using very large scalable and virtualized resources over the Internet. Various definitions and interpretations of "clouds" and "cloud computing" exist. With particular respect to the various usage scopes the term is employed to, we will try to give a representative set of definitions as recommendation towards future usage in the cloud computing related research space. We try to capture an abstract term in a way that best represents the technological aspects and issues related to it. In its broadest form, we can define a 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality of service. To be more specific, a cloud is a platform or infrastructure that enables execution of code services, applications etc. in a managed and elastic fashion. In the Cloud computing use the many type of model like Deployment model and service delivery model. In cloud computing architecture we are use the both type of model. Virtualization technology is the main use in cloud, especially for the cloud infrastructure service. Among the primary drivers for this trend is the ability to aggregate multiple workloads to run on the same set of physical resources, thus resulting in increased server utilization and reduced space and power consumption [1]. In the Cloud computing Scheduling play the vital role. With the help of scheduling we are manage the job of the resource. In the Cloud computing we are use two types of scheduling, static and dynamic scheduling. In the scheduling of the jab we are uses the local and global scheduler for managing the job in Cloud computing.

2. Resource of the Cloud Computing

- Client
- Server
- Switch
- Load Balancer
- Platform
- Software
- Infrastructure
- Datacenter Broker
- Data Information Center

3. Deployment Model of the Cloud-

3.1 Private Cloud

Some vendors have recently use the private cloud because it is a new term to describe private networks on cloud computing. This type of cloud is operated solely for an organization, and it is maintain by the third party and organization. It is use for enterprising datacenter. Private cloud more secures comparison to public Cloud because it is use for internal exposure. Private clouds basically two types, first is On-premise private clouds and second is externally hosted private clouds. Externally hosted private cloud only use for single organization.

3.2 Public cloud

Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web from an off-site

third-party provider who shares resources and bills on a fine-grained utility computing basis.

3.3 Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more security, because it is support the both type of Cloud.

3.4 Community Cloud

The cloud infrastructure is share by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance).Community Cloud is use for sharing the infrastructure between organizations of the same community

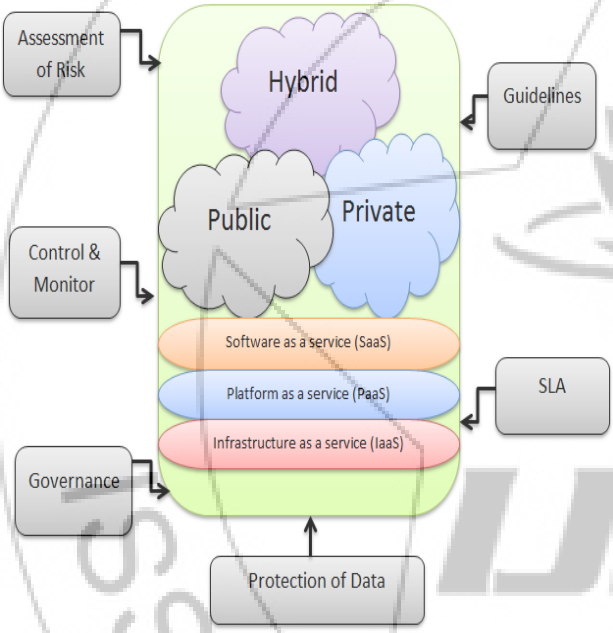

Figure 3.1: Deployment model of the cloud

4. Service Delivery Model

4.1 IAAS

IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

4.2 PAAS- Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks
such as cloud malware[2].

4.3 SAAS- Software as a service (SaaS)

SaaS is a software application delivery model in which enterprises hosts and operates their application over the internet so that customers can access it. Earlier, companies have run software on their own internal infrastructures and computer networks, but now most of them have migrated to the SaaS model. One benefit of this model is customers do not need to buy any software licenses or any additional equipment for hosting the application. Instead, they pay for using the software application. Users checking mail using Gmail, Yahoo mail, managing appointments with Google calendar are some of the SaaS applications users encounter in their daily life. Software-as-a-Service is a software distribution model in which applications are hosted by vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular [2].

4.4 Classification on the basis of Service Providing

- Storage as a service
- Database as a service
- Hardware as a service
- Information as a service
- Software as a service
- Process as a service
- Business as a service
- Application-as-a-service
- Platform-as-a-service
- Integration-as-a-service
- Security-as-a-service
- Governance-as-a-service
- Testing-as-a-service
- Infrastructure-as-a-service

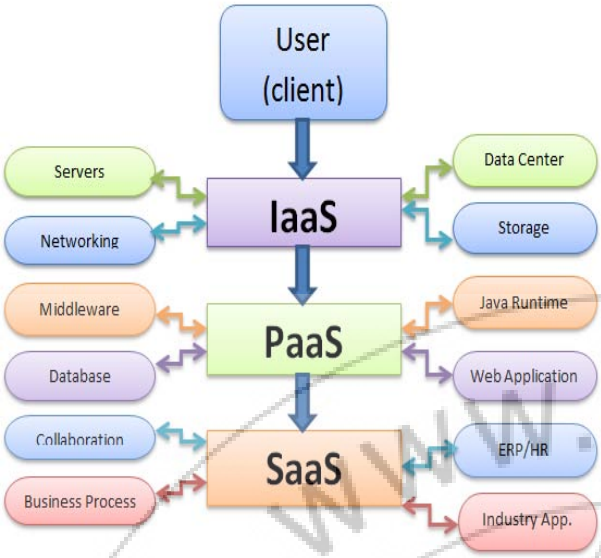

Figure 4.1: Service delivery model

5. Characteristics

5.1 Resource Sharing

Resource sharing based on sharing of resources by different user in a same level of network having same resources.

5.2 Resource Pooling

The provider's computing resources are pooled together to compiled multiple customers using multiple models, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services.

5.3 Multi Tenacity

Cloud computing addressed with the help of Cloud Security Alliance. It indicates the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure [7].

5.4 On demand self services

Computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS [7].

5.5 Scalability

Scalability can be defined in terms of users and storage which maintain scalable property of cloud computing, scalability improves the quality of services in cloud computing and maintain the portion of their scalable system in clouds.

5.6 Flexibility

Maintains the number of resources used by the users in terms of increasing or decreasing the resource. Flexibility improvement depends on the resources used in the cloud which also improves the QOS in cloud computing.

5.7 Pay as you used

This property based on the resources used by the user in terms of their cost, means how much you the resources you have to pay according to that estimated cost.

6. Security Issues

Cloud computing security, performance and availability are three hot spots of the cloud computing research. And cloud computing security is at the top of them. Based on the three different definitions of cloud computing such as IaaS, PaaS and SaaS, cloud computing can be divided into three levels: the infrastructure layer, platform services layer, application layer software [3].

6.1 Failures in Provider Security

In a cloud environment, all security depends on the security of the cloud provider. They control the hardware and the hypervisors on which data is stored and applications are run [4].

6.2 Attacks by Other Customers

The cloud environment is shared among customers. If the barriers between customers break down, one customer can access another customer's data or interfere with their applications [4].

6.3 Traditional Security Issues

Traditional security issues involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company.

6.4 Virtual Machine Level Attack

Vulnerabilities have appeared in VMware (Security Tracker: VMware Shared Folder Bug), Xeon (Xeon Vulnerability), and Microsoft's Virtual PC and Virtual Server (Microsoft Security Bulletin MS07-049). Vendors such as Third Brigade mitigate potential VM-level vulnerabilities through monitoring and firewalls.

6.5 Cloud service providers vulnerabilities

Platform-level, such as an SQL-injection or cross-site scripting vulnerability. For instance, there have been a couple of recent Google-Docs vulnerabilities (Microsoft Security Bulletin MS07-049). IBM has repositioned its Rational Ashcan tool, which scans for vulnerabilities in web services as a cloud security service (IBM Blue Cloud Initiative).

6.6 Expended Network Attack Surface

The cloud user must secure the infrastructure for the connection because the task may difficult by the cloud being outside the firewall in many cases, it also describes that how the cloud might be attacked by the machine.

6.7 Forensics in the cloud

In cloud computing the data being removed, overwritten, deleted or destroyed by the perpetrator in this case is low. More closely linked to a cloud computing environment would be businesses that own and maintain their own multi-server type infrastructure, though this would be on a far smaller scale in comparison. However, the scale of the cloud and the rate at which data is overwritten is of concern.

6.8 Third Party Data Control

The supported implications of data and applications being held by a third party are difficult and not well understood. There is also a lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation-independent, but in reality, regulatory compliance requires transparency into the cloud. Various security and data privacy issues are prompting some companies to build clouds to avoid these issues and yet retain some of the benefits of cloud computing the following concerns need to be addressed properly [7].

6.9 Contractual obligations

One problem related to infrastructure besides the uncertain alignment of interests is that there might be surprising legal implications. For instance, a passage from amazon's terms of use is as followed "Non-assertion" during and after the term of the agreement, with respect to any of the services that you elect to use, you will not assert nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, end users, vendors, business partners including third party sellers on websites operated by or on behalf of us, licensors, sub-licensees, or transferees, any patent infringement or other intellectual property infringement claim with respect to such Services." This could be determined that after one uses E2C, one cannot file infringement claims against Amazon.

6.10 Auditability

Audit difficulty is another problem of the lack of control in the cloud. Is there sufficient transparency in the operations of the cloud provider for auditing purposes? Currently, this transparency is provided by documentation and manual audits. Defining an on-site audit in a distributed and dynamic multi-tenant computing environment spread all over the globe is a major challenge. Certain regulations will require data and operations to remain in certain geographic locations [7].

7. Current Cloud Security Issue

7.1 Denial of service attack

Availability is a primary concern to cloud customers, it is equally of concern to the service providers who must design solutions to mitigate this threat, denial of service (DoS) has been associated with network layer distributed attacks flooding infrastructure with excessive traffic in order to cause critical components to fail. Within a multi-tenant cloud infrastructure, there are more specific threats associated with DoS. Some of these threats are: Shared resource consumption that include attacks that deprive other customers of system resources such as thread execution time, memory, storage requests and network interfaces can cause a targeted DoS, Virtual machine and hypervisor exploitation, attacks that exploit vulnerabilities in the underlying operating system hosting a virtual machine instance will allow attackers to cause targeted outages or instability. Attacks using these methods are designed to circumvent traditionally well-defined cloud architecture that has concentrated on securing against external network-based DoS attacks [7].

7.2 Mobile Device Attack

In now days there are the markets of smart phones in the world ,if smartphones increases so now cloud are not limited to laptop or computer devices, attacks are the emerging problems in now a days that are targeted to mobile world.

7.3 Social Networking Attacks

In recent years there is increased popularity of business and social networking sites that also create emerging attacks Attackers can setup identities to gain trust, and use online information to determine relationships and roles of staff to prepare their attacks. A combination of technical attack and social engineering attacks can be deployed against a target user by taking advantage of the people they know and the online social network they use.

7.4 Cheap Data and Data analysis

The advent of cloud computing has creating many data sets for example Google, Collection and analysis of data is now possible cheaply, even for companies lacking Google's resources. The availability of data and cheap data mining techniques have high impact on the privacy of user data, The attackers have massive, centralized databases available for analysis and also the raw computing power to mine these databases. Because of privacy concerns, enterprises running clouds for collecting data are increasingly finding the requirement of anonym zing their data.

7.5 Security Risk Find by This Formula-With the help of this formula we decide that the risk of the event [5].

Risk = Probability of the occurrence of adverse event *Impact of the adverse event.

8. Comparison Between Physical and Virtual Security

8.1 Physical Security

Providers multiple solution in a Security, provide specialized hardware solution to the security, not depends upon the changing environment of virtualization policies limited to the implementation of the security. Physical security based on three factors:

Costly	Complex	Rigid

8.2 Virtual Security

Virtual security provide Single framework for vast security, also provide simplified and relevant visibility for security teams, virtual security followed the property "program once run everywhere" virtual security provide rapid correction of the security. Virtual security based on three factors:

Cost Effective	Simple	Adaptive

9. Scheduling

Scheduling is the most important part of the Cloud computing. In the present time scheduling is biggest concept of the Cloud computing. In scheduling we are managing the process that is called process scheduling and handle the job of the process is called job scheduling. In the job scheduling we use to allocate certain jobs of the particular resources in particular time. In the Cloud computing system we are scheduling the process with the help of many algorithms and many techniques. There are different types of scheduling based on different criteria, such as Static vs. Dynamic, Centralize vs. Distributed, Online vs. Offline [6]. They are defined blow:

9.1 Static Scheduling

Static scheduling is pre-schedule jobs, In this job all information are known about available resource and task and task is assigned once to a resource. In the static scheduling we are decide first that how to schedule the job, and according to the plan the job is schedule with the help of scheduler.

9.2 Dynamic Scheduling

It is more flexible than static scheduling, because it is determining rum time in advance. In the dynamic scheduling we are not pre-schedule that how to schedule the job, So It is decide in the running time environment. Jobs are dynamically available for scheduling over time by the scheduler. It is more critical in the case of load balancing.

9.3 Centralized Scheduling

Centralize scheduling is depend on the scheduler. Centralize/distributed schedulers have the responsibility to make global decision. Centralized scheduling providers the main benefits are ease to implement, efficiency and more control and monitoring on resource.

9.4 Distributed and Decentralize Scheduling

This type of scheduling is use the local schedulers, which are manage the request and maintain the job state of the queue. It has the less efficiency comparison to Centralize Scheduling, because it is use the local scheduler and some other reason.

9.5 Pre-Emptive Scheduling

Pre-Empty Scheduling allows the interrupted job in the execution time. It is support the interrupted job and this type of job is not migrating original resource. It is migrate to another resource. Pre-Emptive Scheduling Support the priority of the resource. So it is more helpful in comparison to another.

9.6 Non Pre-Empty Scheduling

In Non Pre-Emptive Scheduling the interrupted Job is not allowing. First it is complete the execution than release the Job. So without Releasing Job the Job is not interrupt in the execution.

9.7 Online mode scheduling

In online scheduling scheduler play the important role, the scheduler schedule the recent job which is arrive the available resource and this is not waiting to the another/ next time interval of the available resource.

9.8 Offline mode scheduling

In the offline mode scheduling the scheduler store the arriving the job and all arriving job store as a group of problems and then to be solved in successive time intervals.

Comparison

Name	*Method*	*Cost complexity*	*Time*	*Speed*	*Dynamic*	*Static*
Round Robin Algorithm	Batch Mode	No	Yes	No	No	Yes
Job Scheduling Algorithm	Batch Mode	No	Yes	Yes	No	yes
Agent Based	Batch Mode	Yes	Yes	No	Yes	No
Two stage Based	Batch Mode	No	Yes	No	No	yes
Deadline based	Batch Mode	No	Yes	No	Yes	No

10. Scheduling Process

Scheduling process mainly divided in to three stages:

- Resource discovering and filtering.
- Resource selection.
- Task submission.

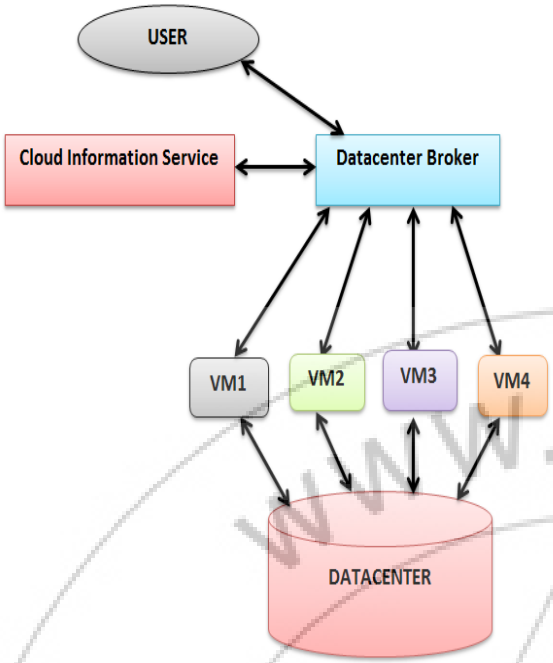

Figure 10.1: Scheduling Process

11. Conclusion

Scheduling is one of the most important tasks in cloud computing environment. In this paper we have analyze various scheduling algorithm and managing the job/task. In this paper our work based on the scheduling. We are describing in this paper many scheduling. Multilevel scheduling is most important or very useful for the cloud computing to managing the process. So we are use the multilevel scheduling method. It is best scheduling method for cloud computing environment. In multilevel scheduling method we categorize the task in different level. In the first level we are filter the task and in the second level select and execute the task. With the help of multilevel scheduling we are manage the migration of the process with the efficient result. In this paper the request is performed by the user, certain parameters are defined with each user request, these parameters includes the arrival time, process time, deadline and the input output requirement of the processes.

Reference

[1] **Ying Chen. et al. "Reliable Migration Module in Trusted Cloud based on Security Level - Design and",** International Parallel and Distributed Processing Symposium Workshops & PhD Forum IEEE 2012.

[2] **Kuyoro S. O. et al. "Cloud Computing Security Issues and Challenges",** International Journal of Computer Networks (IJCN), Volume-3, issue no. 5, 2011.

[3] **Zhang Xin. et al. "Research on Cloud Computing Data Security Model Based on Multi-dimension",** International Symposium on Information Technology in Medicine and Education IEEE 2012.

[4] **Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment**, " Ashutosh Kumar Dubey 1 , Animesh Kumar Dubey 2 , Mayank Namdev3, Shiv Shakti Shrivastava4 ".Department of CSE, Assistant Professor, Trinity Institute of Technology and Research, Bhopal.

[5] **Swetha Reddy Lenkala and Sachin Shetty . "Security Risk Assessment of Cloud Carrier",** International Symposium on Cluster, Cloud, and Grid Computing IEEE/ACM 2013.

[6] **Pinal Salot "A Survey of Various Scheduling Algorithm in Cloud Computing Environment",** International Journal of Research in Engineering and Technology (IJRET), Volume-2, issue no.2, pp. 131-135, Feb. 2013.

[7] **K.Geetha. et al. "Survey for security issues in the cloud computing data",** International Journal of Advances In Computer Science and Cloud Computing, (ISSN), Volume-1,issue no.2, Nov. 2013.