IDHAYA COLLEGE FOR WOMEN
KUMBAKONAM - 612 001

PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE

ACADEMIC YEAR	:	**2019-2020**
SEMESTER	:	**IV**
CLASS	:	**II M.Sc (CS)**
SUBJECT INCHARGE	:	**Dr. C.PREMILA ROSY**
SUBJECT NAME	:	**CLOUD COMPUTING**
SUBJECT CODE	:	**P16CS41**

UNIT V

MONITORING AND MANAGEMENT

An Architecture for Federated Cloud Computing - Introduction – A typical Usecase – The Basic Principles of Cloud Computing – A Federated Cloud Computing Model – Security Considerations – Service Providers Perspective of SLA Management in Cloud Computing: - Traditional Approaches to SLO Management – Types of SLA – Life Cycle of SLA – SLA Management in Cloud –Automated Policy-based Management – Performance Prediction for HPC on Clouds: - Introduction – Background –Grid and Cloud – Performance related issues of HPC in the Cloud.

BASIC PRICIPLES OF CLOUD COMPUTING

- Cloud computing works more as a service provider for utilizing computer resource.
- Cloud computing is a centralized model.
- Cloud is a collection of computers usually owned by a single party.
- Cloud offers more services all most all the services like web hosting, DB (Data Base) support and much more.
- Cloud computing is typically provided within a single organization (eg : Amazon).

There are certain measures which can improve privacy in cloud computing.

1. The administrative staff of the cloud computing service could theoretically monitor the data moving in memory before it is stored in disk. To keep the confidentiality of a data, administrative and legal controls should prevent this from happening.
2. The other way for increasing the privacy is to keep the data encrypted at the cloud storage site, preventing unauthorized access through the internet; even cloud vendor can't access the data either.

A FEDERATED CLOUD COMPUTING MODEL

The view of EGI Federated Cloud

- The European Grid Infrastructure (EGI) is a federation of national and domain specific resource infrastructure providers, who wish to use virtualized management environments to improve the local delivery of services.
- Many of EGI's current and new user communities would also like to access the flexibility provided by virtualization across the infrastructure resulting in a cloud-like environment.
- Federating these individual virtualized resources has been a major priority for EGI, therefore it has set up the Federated Clouds Task Force.
- Its main objectives were to provide a guideline for its resource providers to securely federate and share their virtualized environments as part of the EGI production infrastructure, and to create a testbed to evaluate the integration of virtualized resources within the existing EGI production infrastructure for monitoring, accounting and information services.
- Their guidelines do not define what hypervisor the participating resource providers should use, and the federation adopts a set of well-defined functionalities and interfaces that every provider is free to implement independently.

Inter-Cloud and Cloud federation approaches

- Cloud federation refers to a mesh of cloud providers that are interconnected based on open standards to provide a universal decentralized computing environment where everything is driven by constraints and agreements in a ubiquitous, multi-provider infrastructure.
- Until now, the cloud ecosystem has been characterized by the steady rising of hundreds of independent and heterogeneous cloud providers, managed by private

subjects, which offer various services to their clients.

- In this subsection next to the already overviewed research projects, we gather relevant federative approaches found in the literature.
- Cloud providers offering PaaS solutions may form "sub-federations" simultaneously to these approaches.

InterCloud vision

- Cloud Computing will be the 5th utility by satisfying the computing needs of everyday life.
- Their pioneer paper discusses the current trends in Cloud computing and presents candidates for future enhancements.
- They emphasize the market-oriented side of Clouds, and introduce a market-oriented cloud architecture, then discuss how global cloud exchanges could take place in the future.
- They further extended this vision by [24] suggesting a federation oriented, just in time, opportunistic and scalable application services provisioning environment called InterCloud.
- They envision utility oriented fede- rated IaaS systems that are able to predict application service behavior for intelligent down and up-scaling infrastructures.
- They list the research issues of flexible service to resource mapping, user and resource centric QoS optimization, integration with in-house systems of enterprises, scalable monitoring of system components.
- They present a market-oriented approach to offer InterClouds including cloud exchanges and brokers that bring together producers and consumers.
- Producers are offering domain specific enterprise Clouds that are connected and managed within the federation with their Cloud Coordinator component.

Multi-Cloud approach

- Two use case scenarios that exemplify the problems of multi-cloud systems like (i) VM mobility where they identify the networking, the specific cloud VM management interfaces and the lack of mobility interfaces.
- As the three major obstacles and (ii) storage interoperability and federation scenario in which storage provider replication policies are subject to change when a cloud provider initiates subcontracting.
- They offer interoperability solutions only for low-level functionality of the clouds that are not focused on recent user demands but on solutions for IaaS system operators.

FCM approach

- Albeit this does not mean that different IaaS providers may not share or rent re-sources, but if they do so, it is transparent to their higher-level management.

- Such a federation can be enabled without applying additional software stack for providing low-level management interfaces.

- The logic of federated management is moved to higher levels, and there is no need

for adapting interoperability standards by the participating infrastructure providers, which is usually a restriction that some industrial providers are reluctant to undertake.

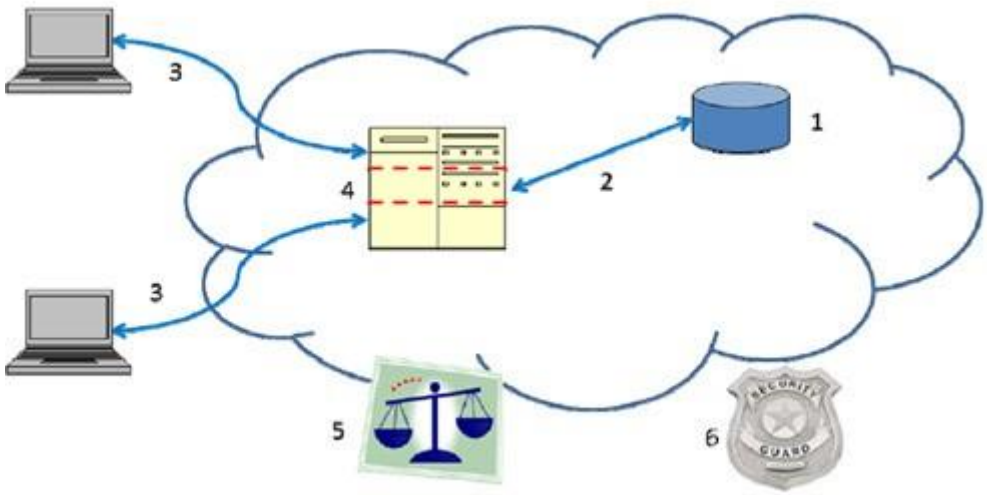
SECURITY CONSIDERATIONS

CLOUD COMPUTING SECURITY AND PRIVACY ISSUES

- There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.
- Therefore, security issues for many of these systems and technologies are applicable to cloud computing.
- For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns.
- For example, mapping the virtual machines to the physical machines has to be carried out securely.
- Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing.
- In addition, resource allocation and memory management algorithms have to be secure.
- Finally, data mining techniques may be applicable for malware detection in the clouds an approach which is usually adopted in *intrusion detection systems* (IDSs).

These six areas are:

(1) security of data at rest
(2) security of data in transit
(3) authentication of users/applications/ processes
(4) robust separation between data belonging to different customers
(5) cloud legal and regulatory issues
(6) incident response.

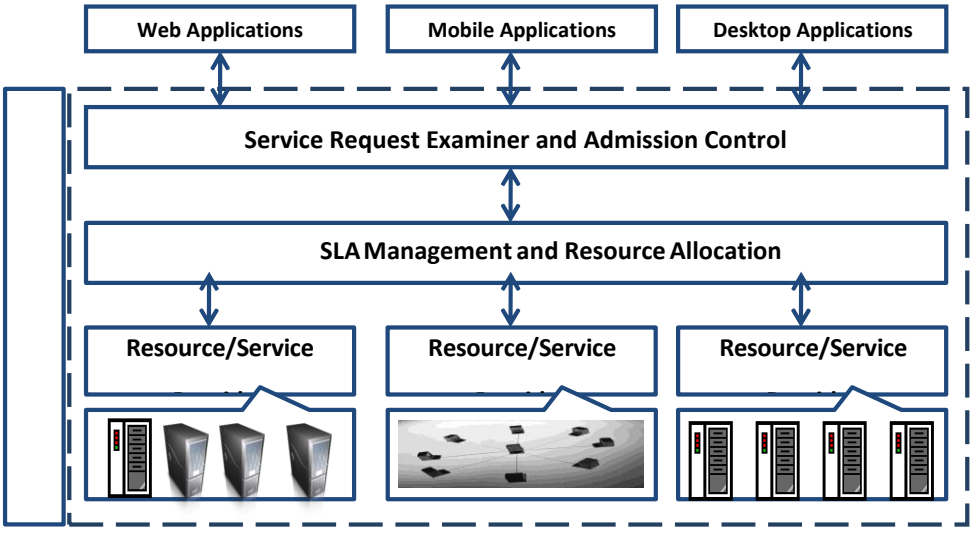


SERVICE PROVIDERS PERSPECTIVE OF SLA MANAGEMENT IN CLOUD COMPUTING

SLAs are used to identify parties who engage in the electronic business, computation, and outsourcing processes and to specify the minimum expectations and obligations that exist between parties.

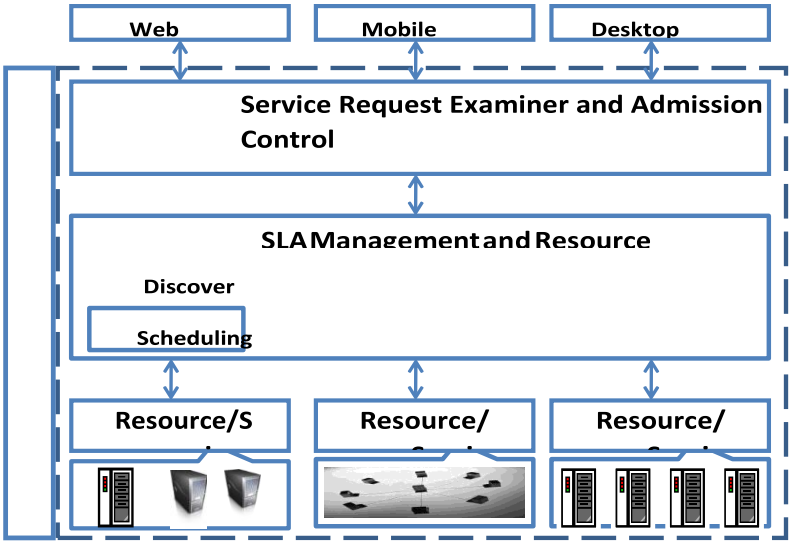
The most concise SLA includes both general and technical specifications, including business parties, pricing policy, and properties of the resources required to process the service (Yeo et. al. 2006). According to Sun Microsystems Internet Data Center Group"s report (2002), a good SLA sets boundaries and expectations of service provisioning and provides the following benefits:

- **Enhanced customer satisfaction level:** A clearly and concisely defined SLA increases the customer satisfaction level, as it helps providers to focus on the customer requirements and ensures that the effort is put on the right direction.
- **Improved Service Quality:** Each item in an SLA corresponds to a Key Performance Indicator (KPI) that specifies the customer service within an internal organisation.
- **Improved relationship between two parties**: A clear SLA indicates the reward and penalty policies of a service provision. The consumer can monitor services according to Service Level Objectives (SLO) specified in the SLA. Moreover, the precise contract helps parties to resolve conflicts more easily.



Utility Architecture

The layered architecture of a typical utility computing system is shown in *Figure 2*. From top to bottom it is possible to identify four layers, a User or Broker submits its requests using various applications to the utility computing system, the Service Request Examiner is responsible for admission control, SLA Management balances workloads, and a Resource or Service Provider offers resources or services.

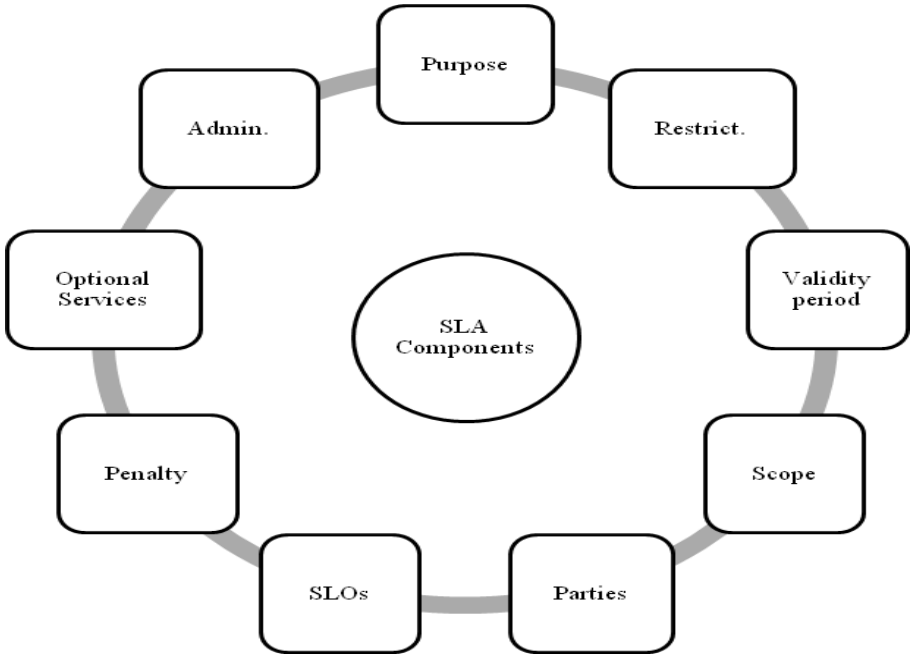


Area	Definition	Source
Web Services	"SLA is an agreement used to guarantee web service delivery. It defines the understanding and expecta- tions from service provider and service consumer".	HP Lab (Jin et. al. 2002)
Networking	"An SLA is a contract between a network service pro- vider and a customer that specifies, usually in mea- surable terms, what services the network service pro- vider will supply and what penalties will assess if the service provider can not meet the established goals".	Research Project
Internet	"SLA constructed the legal foundation for the service delivery. All parties involved are users of SLA. Ser- vice consumer uses SLA as a legally binding descrip- tion of what provider promised to provide. The ser- vice provider uses it to have a definite, binding record of what is to be delivered".	Internet NG (Ron et.al.2001)
Data Center Management	"SLA is a formal agreement to promise what is possi- ble to provide and provide what is promised".	Sun Microsystems Internet Data Center group (2002)

SLA Components

An SLA defines the delivery ability of a provider, the performance target of consumers‟ requirement, the scope of guaranteed availability, and the measurement and reporting mechanisms (Rick, 2002).

- **Purpose**: Objectives to achieve by using an SLA.
- **Restrictions**: Necessary steps or actions that need to be taken to ensure that the requested level of services are provided.
- **Validity period:** SLA working time period.
- **Scope**: Services that will be delivered to the consumers, and services that will not be covered in the SLA.
- **Parties**: Any involved organizations or individuals involved and their roles (e.g. provider and consumer).
- **Service-level objectives (SLO)**: Levels of services which both parties agree on. Some service level indicators such as availability, performance, and reliability are used.
- **Penalties:** If delivered service does not achieve SLOs or is below the performance measurement, some penalties will occur.



- **Optional services**: Services that are not mandatory but might be required.
- **Administration**: Processes that are used to guarantee the achievement of SLOs and the related organizational responsibilities for controlling these processes.

TRADITIONAL APPROACHES TO SLO MANAGEMENT

TYPES OF SLA

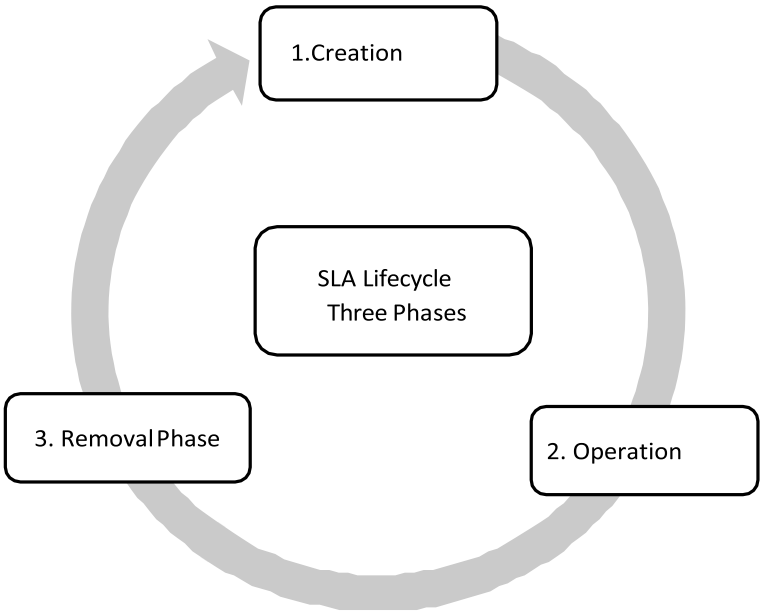
Three types:

i. Service based SLA
ii. Customer based SLA
iii. Multi-level or Hierarchical SLA

LIFE CYCLE OF SLA

SLA Lifecycle

- Firstly, the **creation phase,** in which the customers find service provider who matches their service requirements.
- Secondly, the **operation phase,** in which a customer has read-only access to the SLA.
- Thirdly, the **removal phase,** in which SLA is terminated and all associated configuration information is removed from the service systems.



- A more detailed life cycle has been characterized by the Sun Microsystems Internet Data Center Group (2002).

Which includes six steps for the SLA life cycle:

- The first step is **'discover - service providers'**, in where service providers are located according to consumer‟s requirements.
- The second step is **'define – SLA',** which includes definition of services, parties, penalty policies and QoS parameters.
- In this step it is possible to negotiate between parties to reach a mutual agreement. The third step is **'establish agreement',** in which an SLA template is established and filled in by specific agreement, and parties are starting to commit to the agreement.
- The fourth step is **'monitor SLA violation'**, in which the provider‟s delivery performance is measured against to the contract.
- The fifth step is **'terminate SLA'**, in which SLA terminates due to timeout or any party‟s violation.
- The sixth step is **'enforce penalties for SLA violation'**, if there is any party violating contract terms, the corresponding penalty clauses are invoked and executed.

SLA MANAGEMENT IN CLOUD

- Defining service level agreements (SLAs) for cloud services
- Data-as-a-Service (DBaaS) reference architecture

Name	Type	Domain	Dynamic Establish/ Management	Negotiation	Metrics	Define Man- agement Actions	Sup- port Reuse	Provide Type Systems	Define Seman- tic	Cope with SLA life- cycle
Bil ater al Pro toc ol	Java, . Net And Web Service based proto- col	Originall y for resource res- ervation in Grids.	Yes	Yes	Yes	Yes	Yes.	Yes	Support by Web Service.	Step 1 to Step 4.
WS- Agreem ent	XML language; Framewo rk; A protocol	Any domain	Establ ish and mana ge dy- namic ally	Re/neg otiation with WS- Agree ment Negoti ation	Do not de- fine specifi- cation of Metrics associate d with agreeme nt parame ters.	Yes	Yes	Yes	Not for- mally defined	Step 1 to step 6
WSLA	Provide language; Framewo rk; runtime ar- chitecture	Originally for Web services	Establ ish and mana ge dy- namic ally	Re/neg otiation .	Allows crea- tion of new metrics	Yes	Yes	NA	Not for- mally defined	Step 1 to step 6
QML	language	Any Domain	Yes	Yes	Allows crea- tion of new metrics	Yes	Yes	Yes, al- lows de- finition of new t y p e systems	Yes	Step 1 to step 4
WSOL	XML	Originally for Web Services	Yes	Origin ally do not support But support now.	NA	Yes	Yes	Yes	No	Step 1 to step 4
QUO	CORBA specific framework	Any domain	Yes	Yes	NA	Yes	Yes	Yes	No	Step 1 to step 4
SLAng	XML Lan- Guage	Orig nay for Internet DS environm ent	NA	Yes	No But based on behavior of SLA parties	NA	Yes	Yes	Yes	Step 1 to Step 4

- Cloud API requirements
- Business process and information frameworks for cloud
- Secure virtual private cloud reference architecture
- Standard service definitions/SKUs (Taxonomy of services)
- Cloud SDO liaisons
- eTOM and ITIL; how to combine them in a cloud context?
- Cloud service provider benchmarking and metrics
- Billing engine, client billing and partner revenue sharing for cloud services
- Common definition of commercial terms (business contract language)

AUTOMATED POLICY-BASED MANAGEMENT

1. Desired location in areas with protected space and higher energy efficiency
2. Sharing of peak-load capacity among a large pool of users, improving overall utilization
3. Separation of infrastructure maintenance duties from domain-specific application development
4. Significant reduction in cloud computing cost, compared with traditional computing paradigms
5. Cloud computing programming and application development
6. Service and data discovery and content/service distribution
7. Privacy, security, copyright, and reliability issues
8. Service agreements, business models, and pricing policies

PERFORMANCE PREDITION FOR HPC ON CLOUDS

High-Performance Computing

- ✓ For many years, HPC systems emphasize the raw speed performance.
- ✓ The speed of HPC systems has increased from Gflops in the early 1990s to now Pflops in 2010.
- ✓ This improvement was driven mainly by the demands from scientific, engineering, and manufacturing communities.
- ✓ For example, the Top 500 most powerful computer systems in the world are measured by floating- point speed in Linpack benchmark results.
- ✓ However, the number of supercomputer users is limited to less than 10% of all computer users.
- ✓ Today, the majority of computer users are using desktop computers or large servers when they conduct Internet searches and market-driven computing tasks.

High-Throughput Computing

- ✓ The development of market-oriented high-end computing systems is undergoing a strategic change from an HPC paradigm to an HTC paradigm.
- ✓ This HTC paradigm pays more attention to high-flux computing.
- ✓ The main application for high-flux computing is in Internet searches and web services by millions or more users simultaneously.
- ✓ The performance goal thus shifts to measure high throughput or the number of tasks completed per unit of time.
- ✓ HTC technology needs to not only improve in terms of batch processing speed, but also address the acute problems of cost, energy savings, security, and reliability at many data and enterprise computing centers.

GRID AND CLOUD

Cloud Computing	Grid Computing
Cloud computing works more as a service provider for utilizing computer resource	• Grid computing uses the available resource and interconnected computer systems to accomplish a common goal
• Cloud computing is a centralized model	• Grid computing is a decentralized model, where the computation could occur over many administrative model
• Cloud is a collection of computers usually owned by a single party.	• A grid is a collection of computers which is owned by a multiple parties in multiple locations and connected together so that users can share the combined power of resources

• Cloud offers more services all most all the services like web hosting, DB (Data Base) support and much more	• Grid provides limited services
• Cloud computing is typically provided within a single organization (eg : Amazon)	• Grid computing federates the resources located within different organization.

PERFORMANCE RELATED ISSUES OF HPC IN THE CLOUD

Security Issues in Cloud Computing

- ✓ Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements.
- ✓ But since there is no common cloud computing security standard, there are additional challenges associated with this.
- ✓ Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits.
- ✓ In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that security in the cloud meets their own security polices through requirements gathering provider risk assessments, due diligence, and assurance activities (CPNI Security Briefing, 2010).
- ✓ Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises.
- ✓ The same internal and external threats are present and require risk mitigation or risk acceptance.
- ✓ In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and implementing security control in a privately-owned cloud. In particular, we examine the following issues:

- The treats against information assets residing in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- The security risks associated with the cloud, and where relevant considerations of attacks and countermeasures.
- Emerging cloud security risks.
- Some example cloud security incidents.

*************ALL THE BEST*************