


Experiment No. _____

Date : _____

Name : Sanket Chandrashekhar Harvande.

Roll No : 19

Sign : 

Sub : Cloud Computing

Assignment No- 2

Q.1 Discuss the following concepts in the context of Cloud computing :-

→ i) Billing & Metering services :-

Metered billing is an advancement made possible by the increasing number of applications & services being delivered via the cloud. Under a meter-billing pricing model, the cloud based application must be able to track your usage level & automatically calculate a price that matches your usage level.

Organisations using cloud services typically receive daily emails that provide alerts for spending data, usage spikes, sudden & unexpected changes & more. This is called metering.

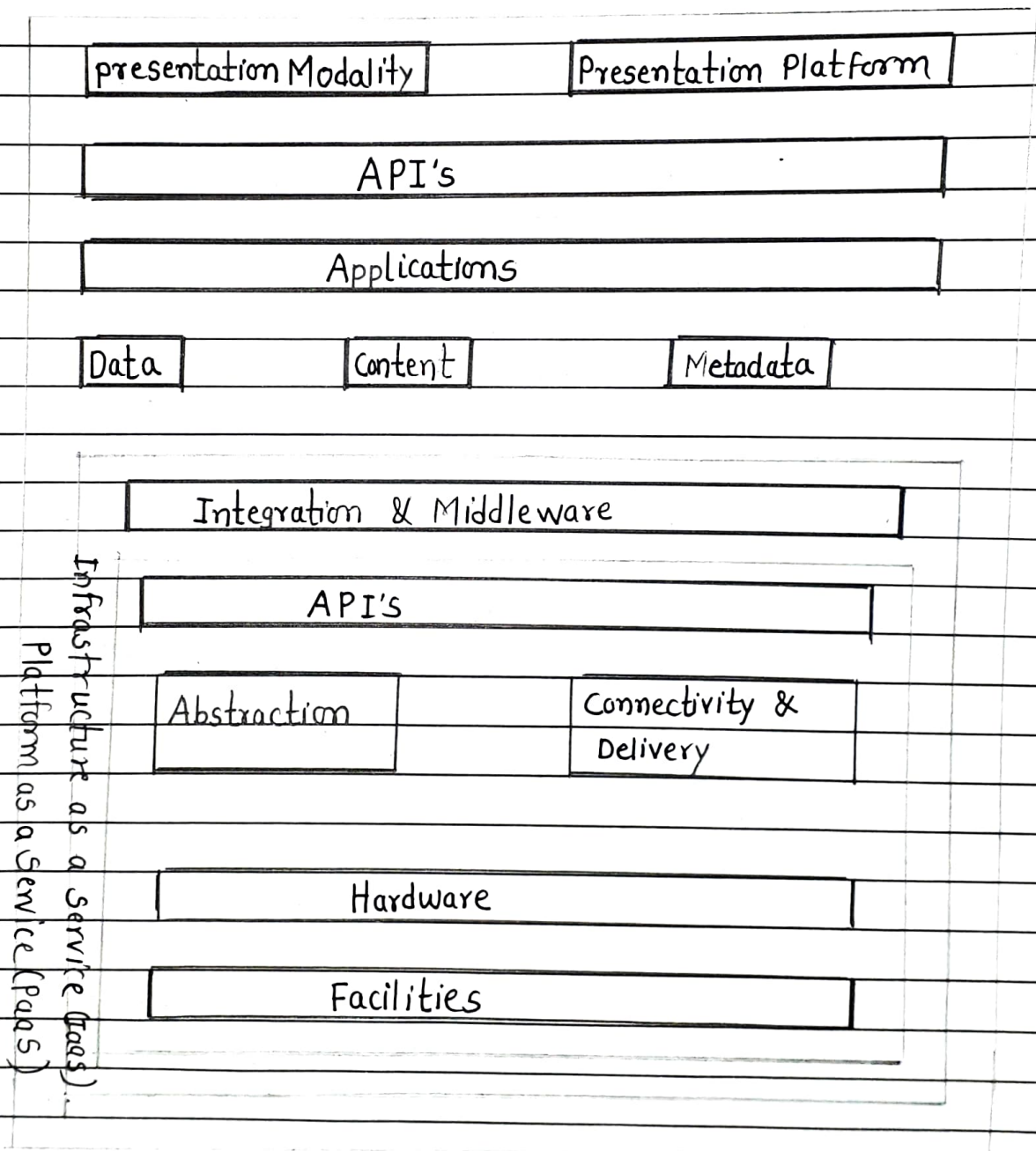
Metered services also called pay-per-use are any type of payment structure in which a customer has access to potentially unlimited resources but only pay for what they actually use.

ii) The cloud security reference model :-

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data

directly, proxy & brokerage service should be employed.

A particular service model defines the boundary between the responsibilities of service provider & customer.



Experiment No. _____

Date : _____

- 1) IaaS is the most basic level of service with PaaS & SaaS next two above level of services.
- 2) Moving upwards, each of the service inherits capabilities & security concerns of the model beneath.
- 3) IaaS provides the infrastructure PaaS provides platform development environment & SaaS provides Operating Environment.
- 4) This model describes the security boundaries at which cloud services providers responsibilities end & the customers responsibilities begin.

Q.2 Prepare a Case study to explore & compare the similar type of services provided by AWS & Azure [Any ten services].

	AWS Service	Azure Service	Description
1)	Elastic compute cloud Instances (EC2)	Virtual machines	Virtual services allow users to deploy, manage & maintain OS & server software.
2)	RDS	SQL Database Database for MySQL Database for PostgreSQL.	Managed relational database services in which resiliency, scale & maintainance are primarily handled by the Azure platform.

	AWS	Azure	Description
3>	AWS Cloudshell	Azure cloud shell.	Azure cloud shells are interactive authenticated browser accessible shell for managing Azure resources.
4>	AWS billing & cost Management	Azure cost management & Billing.	Azure cost management & billing helps us to understand our Azure bill manage our billing account.
5>	Cloudwatch	Application Insights	A feature monitor, application Insights is an extensible application performance management service for developers & identify areas for optimization.
6>	Mobile SDK	App Center	Provides the technology to rapidly build cross-platform & native apps for mobile devices.
7>	Identity & Access Management (IAM)	Azure Active Directory	Allows users to securely control access to services & resources while offering data security & protection.

Date :

AW5	Azure	Description
(8) Server-side encryption with amazon s3 key management service	Azure storage service encryption	Helps us protect & safeguard our data & meet our organization security & compliance commitments.
(9) Simple storage services (S3)	Blob storage	Object storage service for use cases including cloud applications content, backup big data analytics.
10) CloudFront	Content Delivery Network	A global content delivery network that delivers audio, video, applications images & other files.
11) Lightsail	App service	Build, deploy & scale web apps on a fully managed platform.

Q.3

→

Describe google App Engine Architecture & core concepts.

Google App Engine (GAE) is a platform as-a-service product that provides web app developers & enterprises with access to google's scalable hosting & tier 1 Internet service.

Google App Engine is a fully managed services platform that is used to host, build & deploy web application. Users can create a GAE account setup a software development kit & write application source code.

Benefits of GAE :-

• Ease of setup & Use :-

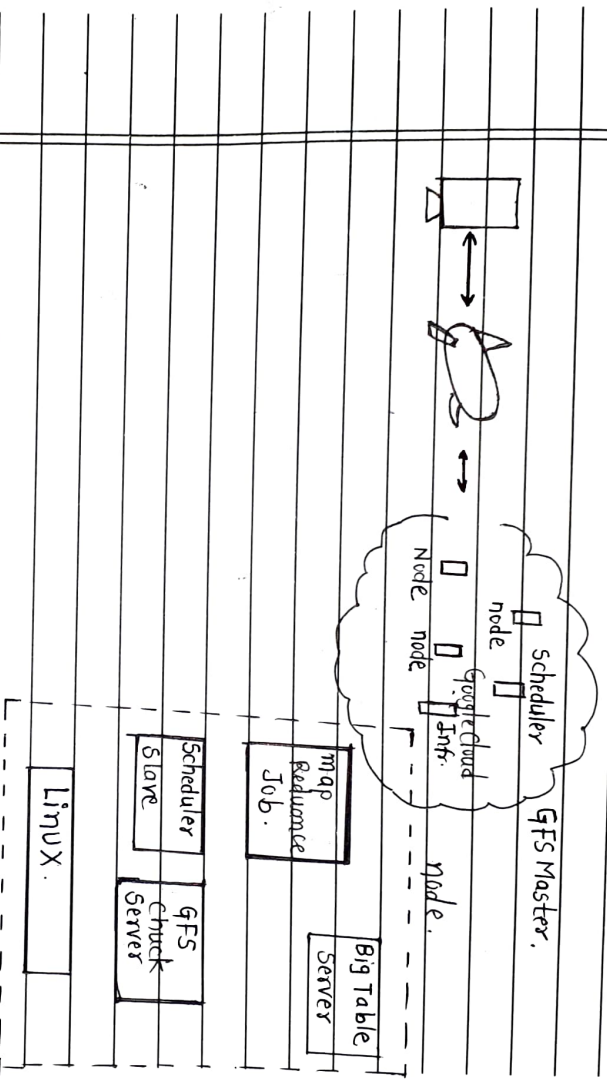
GAE is a fully managed, so users can write code without considering IT operations & back-end infrastructure, Access to application logs also facilitates debugging & monitoring in production.

• Pay-per-use pricing :-

GAE's billing scheme only charges users daily for the resources they use. User can monitor their resources usage & bills on a dashboard.

• Scalability :-

Google App engine automatically scales as workloads fluctuate, adding & removing application instances resources as needed.



Google App engine is one of the earliest PaaS model which is fully scalable & simply a small example, of how high frequency of request can be efficiently handled. Despite the excellent architecture there are too much restrictions which makes the PaaS model inclining towards the projects of SaaS with too much lock in. For example PHP cannot run natively on the App Engine.

Q.4. What are the various & Access Management (IAM) practices followed for authentication authorization & auditing (AAA) of the users accessing cloud Services?

→ Identity & access management (IAM) is perhaps the most important set of security controls. In breaches involving web applications, lost or stolen credentials have been attackers' most used tool for several years running.

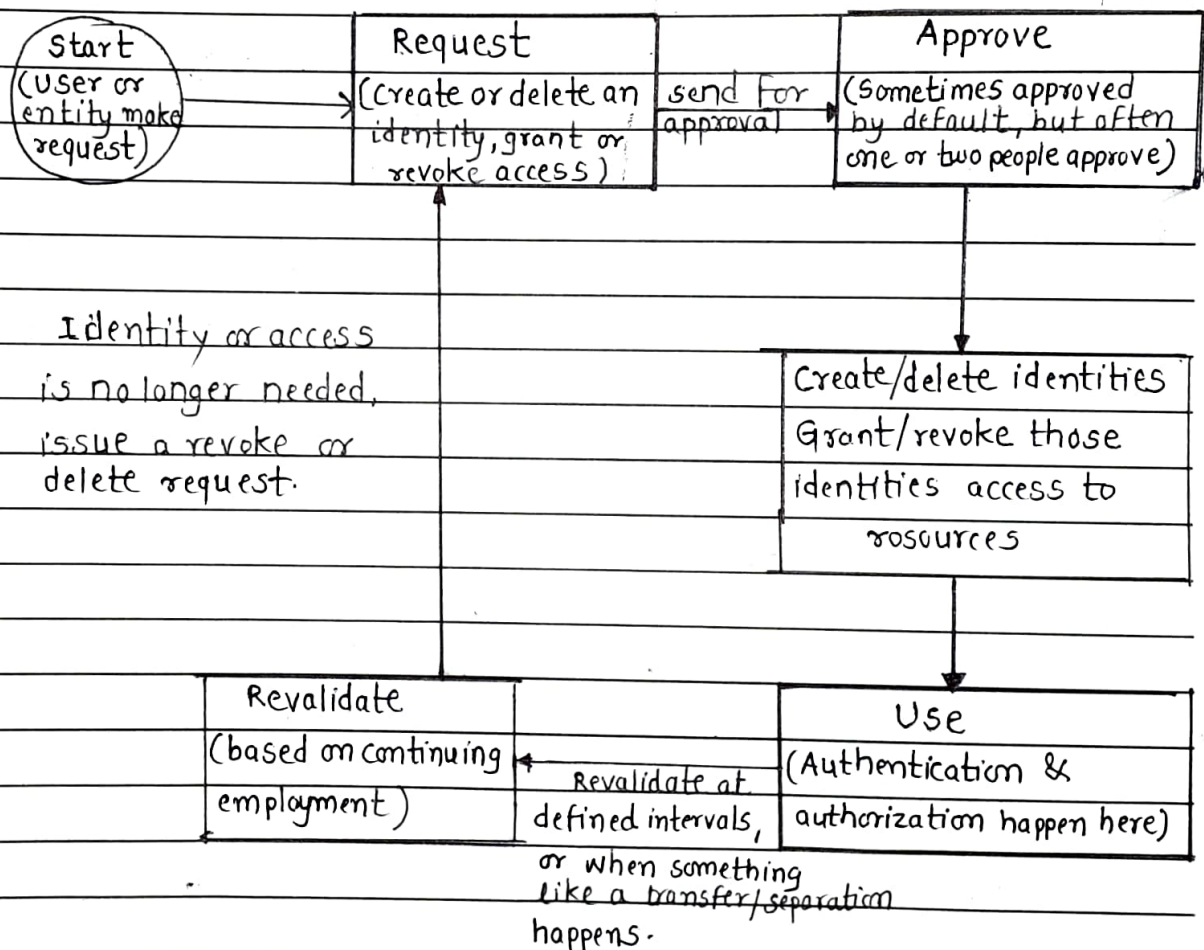


fig: IAM Life Cycle

Experiment No. _____

Date : _____

Authentication :-

It's also important to distinguish between whom you are authenticating. There are often different systems available for :

- Authenticating your organisation's employees with your cloud providers (generally business-to-business & often called something like "Cloud IAM" by cloud providers)
- Authenticating your organisation's customers with your own applications (business-to-consumer)
- Authenticating your organisation's employee with your own applications (business-to-employee).

Authorization :-

End user applications handle authorization themselves.

The most important concepts to remember for authorization are least privilege & separation of duties. As a remainder least privilege means that your users, systems or tools should be able to access only what they need to do their jobs & no more. In practice this usually means that you have a "deny by default" policy in place, so unless you specifically authorize something it's not allowed.

3) Auditing :-

Google cloud services write audit logs that record administrative activities and accesses within your google cloud services. Audit logs helps you answer 'who did what', where & when?' Within your Google Cloud resources with the same level of transparency as in on-premises equipments. Enabling audit logs helps your security auditing and compliance entities monitor Google Cloud data and system for possible vulnerabilities or external data misuse.