UNIT 4: Cloud Solution

Cloud Ecosystem, Cloud Business Process Management, Cloud Service.

Management. Cloud Offerings: Cloud Analytics, Testing Under Control,

Cloud Security: Cloud Information security fundamentals
Cloud security services
Design principles
Secure Cloud Software Requirements
Policy Implementation
Cloud Computing Security Challenges
Virtualization security Management
Cloud Computing Security Architecture.

- The notes have been prepared by using book mention in your syllabus i.e Mastering cloud computing by Buyya, selvi
- To get previous year question paper visit library
- The question that highlighted by yellow color, they should be your top priority for preparation
- As we move more further, I'll be updating the notes.

FAQs

Que: Do I have to use your notes for answer writing.

Ans:

- Nope the notes are prepared for students as for reference material, students who are too busy
- Yes, you can use these notes for answer writing.
- Or you can create your own notes or write answer in your word but it has to be specific
- Do not write YouTube answers or any website answer always follow university syllabus mention book for ref. so you can score more marks.

Cloud ecosystem

To carry any cloud service in market, it needs corresponding pre- investment along with respective metering and charging models in favors of the corresponding business model. For instance, Amazon Elastic Compute Cloud (Amazon EC2) is an ecosystem focused IBM Common Cloud Services Platform or IaaS cloud service. In EC2, the ecosystem artefacts are VMware images. EC2 permits uploading of newly created Virtual Machine (VM) images and charging for these VM images. Each VM instance inherits almost all technical and business decisions already taken by Amazon when they decided to take EC2 to market for a certain price point - on EC2, each VM is running on the basis of availability and performance Service Level Agreements (SLAs) as defined by EC2, the management actions consumers can carry out on the image are predefined by EC2, the metrics that are employed to charge for VMs are the ones defined by EC2, etc. Amazon nails down all these characteristics. For offering EC2, each feature has a effect on the costs. thus, it is not possible to make the features flexible to artefact developers because it would be very difficult to make the corresponding costs flexible. This shows that defining and delivering a cloud service needs nailing down all correspondence functional and non-functional requirements. The artefacts that are developed on top of an ecosystem-focused cloud service have very minimum space to adapt how these functional and non-functional requirements are addressed. It is not to be considered as something negative but rather as something very positive from an ecosystem viewpoint. This is a core value proposition of ecosystem-focused cloud services to offer pretty strict guidelines with respect to how they can be exploited because it is the chief factor driving a reduction in cost of artefact development. The more likely the cloud service is successful, the easier it is to develop artefacts for such a cloud service.

The cloud capability to have multiple environments to deploy the application is a main benefit since it can be a mix and match condition that fits well to the business function and the application. It refers that the organization is able to use multiple solutions for cloud computing. Cloud needs will help to choose the suitable cloud environments based on the business requirements, the application and what the application has to offer.

Benefits of cloud ecosystem

The benefits of cloud ecosystem are as follows -

(i) Services

(ii) Rapid cloud adoption

(iii) Enterprise-wide decision support

(iv) Impact on profit and loss

(v) Single window management and assurance.

Cloud business process management

Business process management conducts an organization's cross- functional, customer focused, end-to-end core business processes. Its pay particular attention to driving overall bottom-line success by integrating verticals and optimizing core work. It gets strategic business goals by directing the deployment of resources from across the organization into efficient processes that generate customer value. Besides, intrinsic to BPM is the principle of 'continuous improvement', perpetually increasing value generation and providing market competitiveness of the organization. It clearly defined and aligns operations, information technology, and organizations.

The cloud environment can help in the following manners -

(i) **Cultural** - During due diligence of the need, cultural considerations of the organization and geographical area should be kept in mind.

(ii) **Continuous** -

(a) Continual enhancement

(b) This relies on longer periods of intervals relating to cloud business.

(iii) **Value-focused Efficiency** -

(a) Bottom-line success

(b) Performance measurement

(c) Customer-centric perspective

(d) Speed at which ROI is delivered.

(iv) **Core Business Integration** -

(a) Holistic

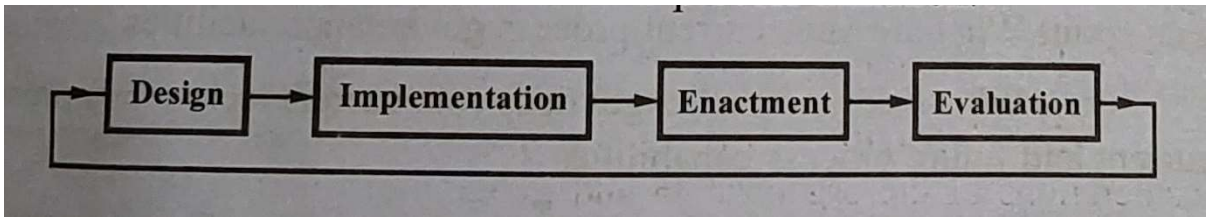
(b) Comprises business and technology

(c) Crosses organizational functions and boundaries.

BPM life cycle

Fig. shows the BPM life cycle which is an iterative process. Each of

the phases of BPM life cycle is as follows -



(i) Design - The business processes within a company are identified in the design phase. The goal of the design phase is to capture the processes in business process models. Then these models can be simulated and validated. The stakeholders get insight into the correctness and suitability of the business process models by validating and simulating the process.

(ii) Implementation - The implementation of business process models can be performed in two ways -

(a) One can choose to create work lists, with well-defined tasks which can then be assigned to workers within the company. This is often the case when no automation is necessary or possible within the business process execution.

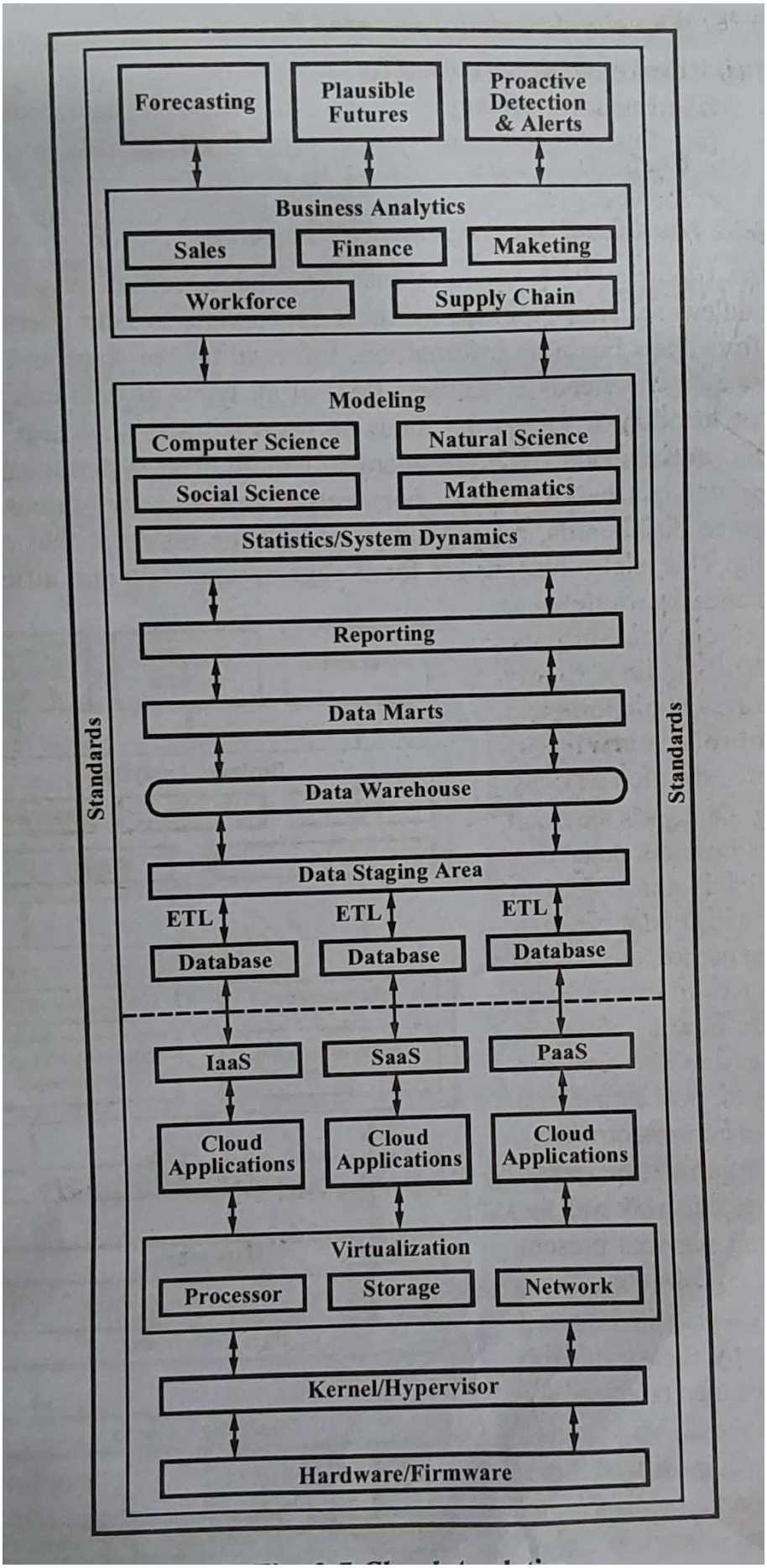
(b) In lot of situations information systems participate in a business process, in which case a business process management system (BPMS) can be used. A BPMS is able to use business process models and create instances of these models for each process initiation.

(iii) Enactment - In this phase the system is used at runtime, so that each initiation of the process is monitored and coordinated by the BPMS. A Process instance is created for each initiation of a process. The most important tool within the enactment phase is the monitoring tool because it provides an overview of the running and finished process instances.

(iv) Evaluation - The monitored information that is collected by the BPMS is used to review the business process in the evaluation phase. The conclusion drawn in the evaluation phase are used as input for the next iteration of the life cycle.

Cloud analytics

The new offering in the new era of cloud computing is cloud analytics. It will ensure the better consequences and will aid in the consulting domain. Cloud analytics offers users with good forecasting technique to explore and optimize the service lines and offer a higher level of accuracy. Cloud analytics can help them apply analytics principles and best practices to explore the various business results and obtain newer levels of optimization. It can merge complex analytics with the newer software platforms and will result in the predictable business circumstance out of every business insight Fig. illustrates a simplified view of cloud analytics.


Forecasting
Plausible Futures
Proactive Detection & Alerts
Business Analytics
Sales
Finance
Maketing
Workforce
Supply Chain
Modeling
Computer Science
Natural Science
Social Science
Mathematics
Statistics/System Dynamics
Reporting
Data Marts
Data Warehouse
Data Staging Area
ETL
ETL
ETL
Database
Database
Database
IaaS
SaaS
PaaS
Cloud Applications
Cloud Applications
Cloud Applications
Virtualization
Processor
Storage
Network
Kernel/Hypervisor
Hardware/Firmware
Standards
Standards

Cloud analytics used

Cloud analytics are used for -

(i) Ensuring privacy

(ii) Ensuring data availability

(iii) Ensuring data quality

(iv) Ensuring data currency

(v) Knowledge process flow.

Cloud analytics working

Cloud analytics operates with the combination of services, hardware and middleware. This expertise makes it appropriate to help clients find new value from their business information. Information software and delivering business analytics needs a seamless flow of all types of data independent of platform, location or format. Its focus on open industry standards is main to this effort and provides us a considerable benefit. The system characteristics include analytics based on text, perspective analytics techniques, business intelligence dashboards, mining activities and the platform that offers data reporting. This is also responsible for storage optimization and different high performance data-warehouse management techniques. This also contain a highly reliable system platform and the umbrella activity of different installation services.

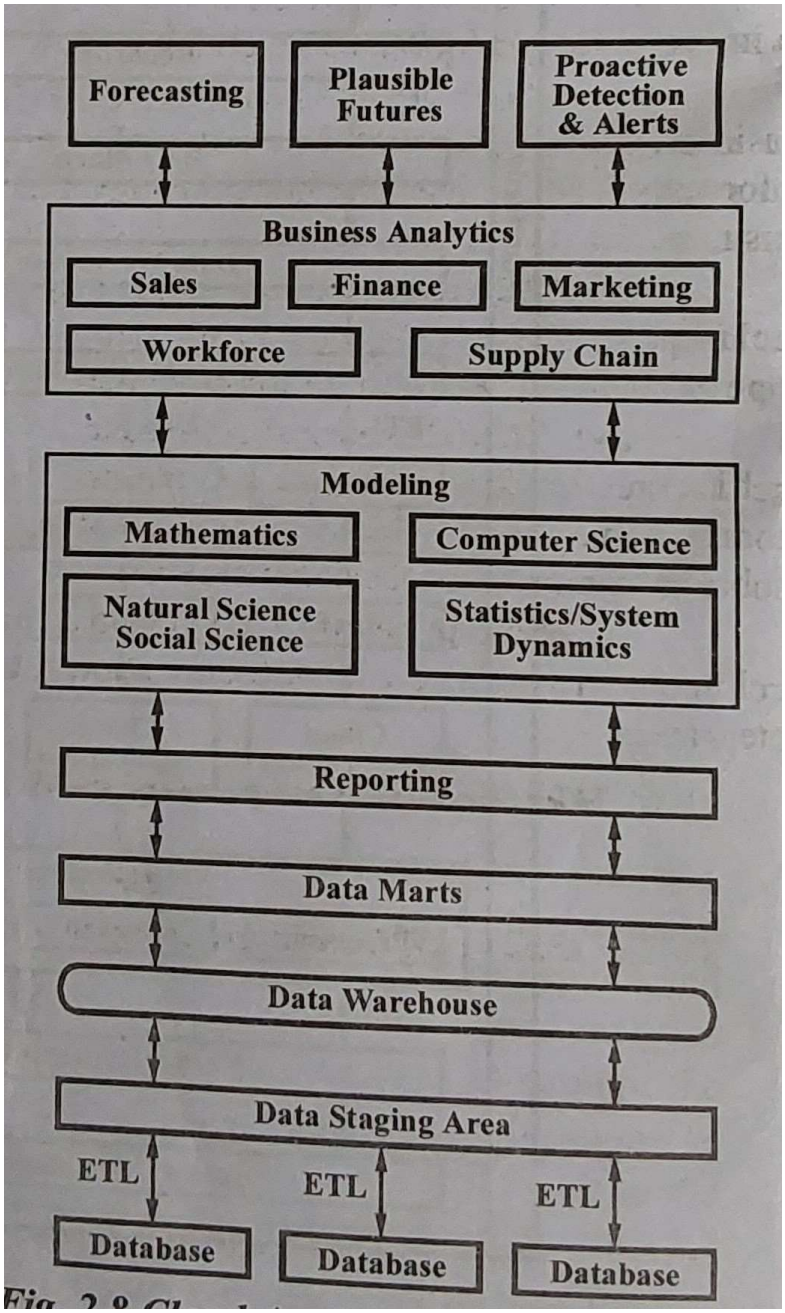


Fig. depicts the cloud analytics business outcomes. Analytics systems help to obtain the right information as and when needed, mention the right sources to obtain it and recognize how to obtain it. Thus, analytics also assists in designing the policies faster on the basis of information present in the organization since decision makers work with the exploration services present inside the organization. It also assists in gauging the business outcomes by measuring the different metrics produced by using analytics. This provides the choice through which the organization can enhance the profitability, minimizes errors and lessen cycle time.

Cloud security

Cloud computing security refer to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment. Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered.

Key mechanism uses to protect data in cloud storage

Or

Data security handled in cloud

Following are the key mechanisms for protecting data -

(i) Access control

(ii) Auditing

(iii) Authentication

(iv) Authorization.

The core technology for protecting data in transmit to and from the cloud as well as data stored in the cloud is encryption. The goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage.

Attributes of cloud security

Cloud security attributes belong to broadly into the following categories

(i) Confidentiality, Privacy and Trust - These are well known basic attributes of digital security such as authentication and authorization information as well as protecting privacy and trust.

(ii) Physical Protection of Enterprise Cloud Assets - This category belongs to protecting enterprise cloud centers and its assets.

(iii) Enterprise Cloud Services Security - This includes security all its services such as SaaS, PaaS and IaaS. This is the key area of attention needed for achieving enterprise cloud security.

(iv) Data Security - This category is again paramount for sustaining enterprise cloud technology. This includes protecting and recovering planning for enterprise cloud data and service centers. It is also important to secure data in transaction

Different cloud security services

Or

Categories of security services provided for information over the cloud

The different cloud security services are as follows -

(i) **Authentication** - Authentication refers to the testing or reconciliation of evidence of a user's identity. It creates the user's identity and makes sure that users are who they claim to be. Consider, for example, that a user provides an identity to a computer login screen and then has to give a password. The computer system authenticates the user by verifying that password belongs to the same user providing the ID.

(ii) **Authorization** - Authorization means the rights and privileges granted to a user that provide access to computer resources and information assets.

(iii) **Accountability** - Accountability means the ability to determine the actions and behaviors of an individual within a cloud system and to recognize that specific

individual. Audit trails and logs help accountability. They can also be used to do postmortem studies in order to analyze historical events and the individuals related with those events.

(iv) **Auditing** - A one-time or periodic event to evaluate security is a system audit. Information technology (IT) auditors are of two types - internal and external. Internal auditors work for a given organization, while external auditors do not. External auditors are certified public accountants or other audit professionals that do an independent audit of an organization's financial statements. Internal auditors have a much broader mandate compared to external auditors, like checking for compliance and standards of due care, auditing operational cost efficiencies, and recommending the suitable controls.

The following functions are audited by IT auditors -

(a) System development standards

(b) System and transaction controls

(c) Backup controls

(d) Data center security

(e) Data library procedures

(f) Contingency plan.

Besides, IT auditors may suggest enhancements to control, and take part in a system's development process to support an organization avoid expensive reengineering after the system's implementation.

Cloud security design principle

The various cloud security design principles are as follows –

(i) **Least Privilege** - This principle requires that an individual, process, or other type of entity should be provided the minimum privileges and resources for the minimum time needed to finish a task. This principle decreases the opportunity for unauthorized access to important information.

(ii) **Separation of Duties** - This principle needs that completion of a particular sensitive activity or access to sensitive objects relies on the satisfaction of a plurality conditions. Consider, for example, an authorization would need signatures of two or more individual, or the arming of a weapons system would need two individuals with distinct keys. Therefore, in order to compromise the system, separation of duties forces collusion among entities.

(iii) **Defense in Depth** - This is the application of multiple layers of protection wherein a subsequent layer will offer protection if a previous layer is broken.

(iv) **Fail Safe** - This refers to that when a cloud system fails it should fail to a state where the security of the system and its data arc not compromised.

(v) **Economy of Mechanism** - This principle promotes easy and comprehensible design and implementation of protection mechanisms, so that unwanted access paths can be identified and removed or do not exist.

(vi) **Complete Mediation** - In this principle, each request by a subject to access an object in a computer system follows an effective and valid authorization procedure. The following are included in the complete mediation -

(a) Identification of the entity requesting for the access

(b) Verification of the request that it has not altered since its initiation

(c) Application of the suitable authorization procedures

(d) The same entity reexamines the previously authorized requests

(vii) **Open Design** - Some think that the encryption algorithm should be kept secret to be harder to break. In contrast, others feel that exposing the algorithm to review and study by experts at large while keeping the encryption key secret results in a stronger algorithm since the experts have a higher probability to find weaknesses in it. Generally, the latter approach is more effective, except in the case of organizations like the National Security Agency (NSA), which uses the best cryptographers and mathematicians. Mostly, an open-access cloud system design offers a more secure authentication method. Security of such mechanisms relies on protecting passwords or keys.

(viii) **Least Common Mechanism** - According to this principle, a minimum number of protection mechanisms should be common to multiple users, because shared access

paths can be sources of unauthorized information exchange. The least common mechanism enhances the least possible sharing of common security mechanisms.

(ix) **Psychological Acceptability** - It means the easy to use and intuitiveness of the user interface that controls and interacts with the cloud access control mechanisms.

(x) **Weakest Link** - The security of a cloud system is as good as its weakest component. Therefore, it is necessary to recognize the weakest mechanisms in the security chain and layers of defense, and enhance them so that risks to the system are alleviated to an acceptable level.

(xi) **Using Existing Components** - In many cases, a cloud implementation security mechanism might not be used to their maximum capability or configured properly. The security posture of an information system will be improved by reviewing the state and settings of the extant security mechanisms and ensuring that they are working at their optimum design points.

One other approach to enhance cloud system security by using existing components is to divide the system into defended subunits. Now, if a security mechanism is used in one sub-unit, it will not affect the other sub-units. This will result in minimum damage to the computing resources.

Different secure cloud requirements

Or

Requirements of secure cloud software

The following three security needs are shared by all software -

(i) It must rely on expected operating conditions, and remain dependable under hostile operating conditions.

(ii) It must be reliable in its own behavior, and in its inability to be compromised by an attacker via exploitation of vulnerabilities or insertion of malicious code.

(iii) It must be resilient enough to recover rapidly to full operational capability with a minimum of damage to itself, the resources and data it handles, and the external components with which it interacts.

Various security benefits on the cloud

(i) Data Encryption - Robust data encryptions within cloud-based security systems have substantially reduced the possibilities of data breaches; these solutions offer a layered approach that consists of security intelligence, key management, and secure access controls. Cloud-based systems give the required freedom to companies to choose their users who will be accessing the data that has been outsourced to the cloud. This way, any attempts to tamper with personal or profession data can be thwarted.

Most companies face the threat of internal data theft by their employees, and stronger access controls can nip these threats in the bud. The multi-layered security features weed out the possibilities of a breach of data to a great extent. Data, irrespective of its type, needs to be protected at all times. Any violations can be hazardous to the goodwill and the functioning of an enterprise.

(ii) Avoid DDoS Attacks - Distributed Denial of Service (DDoS) attacks can result in hefty losses for entertainment companies. Hackers target the website by directing traffic from several sources to the end website, and as a result, the system gets overwhelmed. These DDoS attacks may tarnish the image of the company, as clients begin to lose trust.

Cloud-based security systems guard this imminent threat with real-time scanning of potential risks; this function is further used as a warning tool for various systems which allows for the tracking of incoming threats and attacks instantly - this enables website admins to divert the traffic to several different locations.

(Hi) Regulatory Compliance - Cloud computing security solutions usually provide reliable SOC1 and SOC2 certifications to the entertainment businesses. These certifications ensure periodic scrutiny of data and all types of possible glitches. Cloud-based solutions manage the requisite infrastructure for regulatory compliance and the protection of data. Detailed AWS reports about management of security controls ensure all organizations locus on their business operations, without worrying about compliance requirements.

(iv) Secure Storage - Traditional storage solutions do not provide any protection against possible disasters that have the potential to erase required data from devices. Cloud computing allows the users to store their data safely, thereby negating any mishaps that may affect the equipment.

Cloud storage solutions offer private, public, and hybrid solutions which the businesses may choose as per their requirements. The hybrid cloud storage systems allow the users to keep their data secure in the most effective manner.

(v) Patch Management - The vulnerabilities of a website are often exploited by hackers to breach the security system of a company. Cloud service providers keep their sites up to date; further on, they ensure that no vulnerabilities exist. Moreover, cloud solutions offer real-time assistance to clients by providing companies with the option to scale cloud solutions during high traffic situations. This flexibility allows companies to reduce their cost of services substantially.

These large number of security features are quite flexible, agile, and affordable. Enhanced security features offer sufficient protection to the private and financial data of both media and entertainment companies and help to thwart data and intellectual property breaches. In this era of digitalization, where cybercrime has emerged as a norm, cloud-based solutions seem to be the best alternative to traditional security systems.

Types of security polices

In the corporate world, when we refer to specific policies, rather than a group policy, we generally mean those policies that are distinct from the standards, procedures, and guidelines. Policies are considered the first and highest level of documentation for strategic reasons, from which the lower-level elements of standards procedures, and guidelines flow. The various security policy types are as follows -

(i) **Senior Management Statement of Policy** - This is the first policy of any policy creation process. This high level policy acknowledges the importance of the computing resources to the business model.

(ii) **Regulatory Policies** - These policies are implemented by organization due to compliance regulation, or other legal requirements. These policies are very detailed and specific to the industry where the organization works. These organizations may be financial institutions, public utilities, or some other kind of organization working in the public interest.

(iii) **Advisory Policies** - These policies are not mandated but strongly recommended, perhaps with serious results defined for failure to follow them. An organization following such policies needs most employees to consider these policies mandatory. Most policies belong to this category.

(iv) **Informative Policies** - These policies exist to inform the reader. There are not implied or specified requirements. The audience for this information can be some internal or external parties.

Term policy implementation

A policy is one of those terms that can mean several things. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global information security policy. A good, well written Policy is more than an exercise created on white paper - it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a government or regulatory function. A policy

can also control access to trade secrets. Security policies and their relation hierarchy is show in fig.

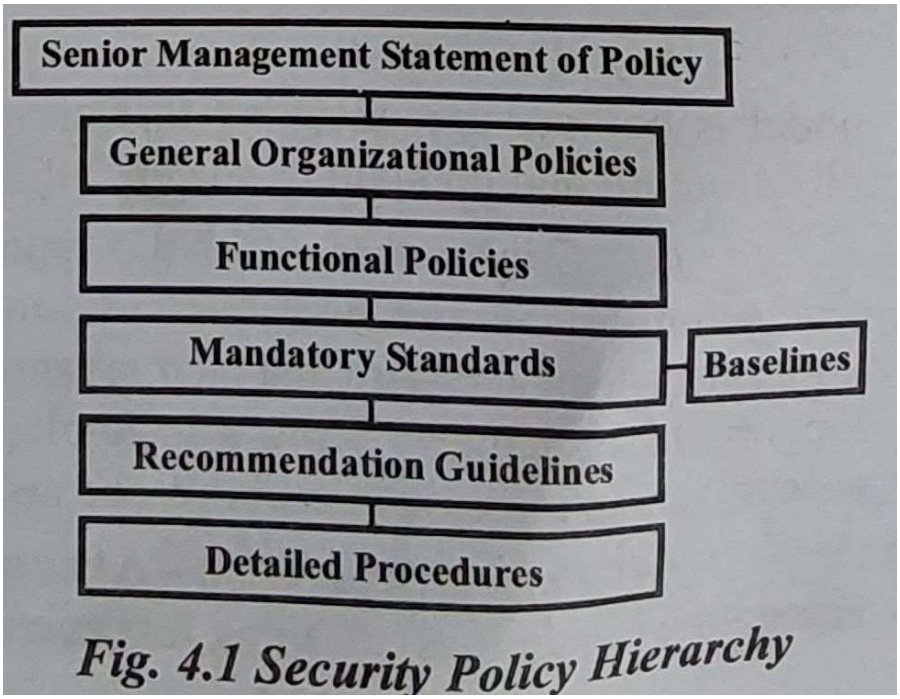


Fig. 4.1 Security Policy Hierarchy

Different area of cloud policy implementation

(iv) Authentication and access control – One of the key cloud security areas is access control and is a good example to demonstrate the shared responsibility concept. Paas and SaaS providers, for instance, can provide authentication for cloud applications developers and users. On the other hand, opportunity exist for cloud subscribers to take ownership of authentication and access control to cloud for tighter integration with their identity and access management systems. Client-side access control is an integral component of their cloud security strategy for IaaS subscribers

(ii) Consistency-An overarching and consistent policy framework is critical for successful cloud security implementation. For example, an excellent design to achieve reliable and dynamic logical separation is to apply zone-based and policy-driven security enforcement. A zone is a group attributes they may include traditional networking parameters such as IP address, network protocols and port numbers. The zone may also contain information such as virtual machine (VM) and custom attributes. Approach such as this help ensure policy consistency in a dynamic cloud environment where VMs typically move around.

(iii) Architecture – The cloud computing architecture generally includes the underlying infrastructure, various service components, and certain pervasive functions such as security and resiliency. Furthermore, cloud security has its own architectural structure.

(iv) Automation – A core tenet of the cloud computing business model is pay-per-use, meaning that elasticity is not only reflected in the infrastructure and computing power, but also in the cost structure.

(v) Governance – Cloud computing represents a dramatic shift to new technologies and new business computing models. Providers and subscribers need to ensure that their organizational governance is up to date to support these changes. From a technology perspective, cloud governance necessitates an increase in visibility and auditing capabilities.

(vi) Logical Separation – A key cloud computing benefit is its elastic computing capabilities, meaning that computing power can be ramped up or dialed down rapidly based on demand. To support such a dynamic business computing model, security should be provisioned in a similar manner. Static and physically oriented security configurations such as VLAN-based security are labor intensive and can hardly keep up

with the fast pace. New approaches are needed to achieve logical separation to secure dynamic and shared environments such as multi-tenancy.

(vii) Scalability and Performance – Scalability and performance are requirements for cloud security because of the potentially massive workloads and stringent security requirements involved. Innovative technologies that can help boost performance while maintaining a high security standard is critical to cloud security implementation.

Cloud computing security challenges

The security challenges in cloud computing are as follows

(iv) **Logical Storage Segregation and Multi-tenancy Security Issues** – Users can store and deliver their data across the globe through Internet using cloud computing. The user does not control, and typically does not even know the location where the data is exactly stored. There is a possibility that user and their competitor's data can reside on the same physical storage device with logical segregation. That's why there is a chances of user's private data to be viewed by the other users. If the data and the information are not protected from other users then it is a major risk for the user to keep their information private in the cloud. In addition, the data is deployed on the cloud service provider's infrastructure on a multitenant model basis. This situation brings the security concerns like who maintains the audit records of the data? Who owns the data ownership and control ownership? To handle such sensitive situations, cloud service provider should ensure proper data isolation.

(ii) **Identity Management Issues** – The advancement of cloud computing based on numerous technical and business models signifies that cloud computing with an appropriate identity management can be considered as a superset of all the corresponding issues from these paradigms and many more. As the traditional identity and access management is still facing so many challenges when considering it for cloud computing, it needs to be more secure. Unlike traditional identity management, simply managing users and services is not sufficient is cloud computing.

(iii) **Insider Attacks** – In cloud computing, one of the major security concerns is that the customer loses direct control over potentially business sensitive and confidential data. This needs more attention because the cloud service provider is outside the trusted domain of customer. The risk of malicious insider is the most dangerous security threats. This threat is intensified for customers of cloud services by the union of infrastructure, services and customers under a single controlling domain, with a huge

lack of transparency in the way the cloud service provider services through its processes and procedures.

(iv) **Virtualization Issues** – Virtualization is a key element for cloud computing to achieve its objective. It can be achieved through a hypervisor. Virtualization of enterprise servers introduces noteworthy security concerns due to aggregation of risks. Associating multiple servers with one host removes the physical separation between servers, increasing the risk of undesirable cooperation of one application with others on the same host. At the same time, if an attacker gets the root to access the hypervisor, then it brings significant threats to the cloud computing. The attacker can gain access to all Guest's OS created on that virtualization server, if the attacker hacks the virtualization host machine.

Virtualization of security management

Threats to the virtualized infrastructure are evolving just as quickly, although the global adoption of virilization is a relatively recent event. The virtual machine, virtual memory manager and hypervisor or host OS are the minimum set of components required in a virtual environment. They comprise virtual environment in a few different ways –

(iv) Type 1 virtual environments are considered full virilization environments and have virtual machine running on a hypervisor that interacts with the hardware.

(ii) Type 2 virtual environments are also considered full virtualization but work with a host OS.

(iii) Para-virtualized environments offer performance gains by eliminating some of the emulation that occurs in full virilization environment^

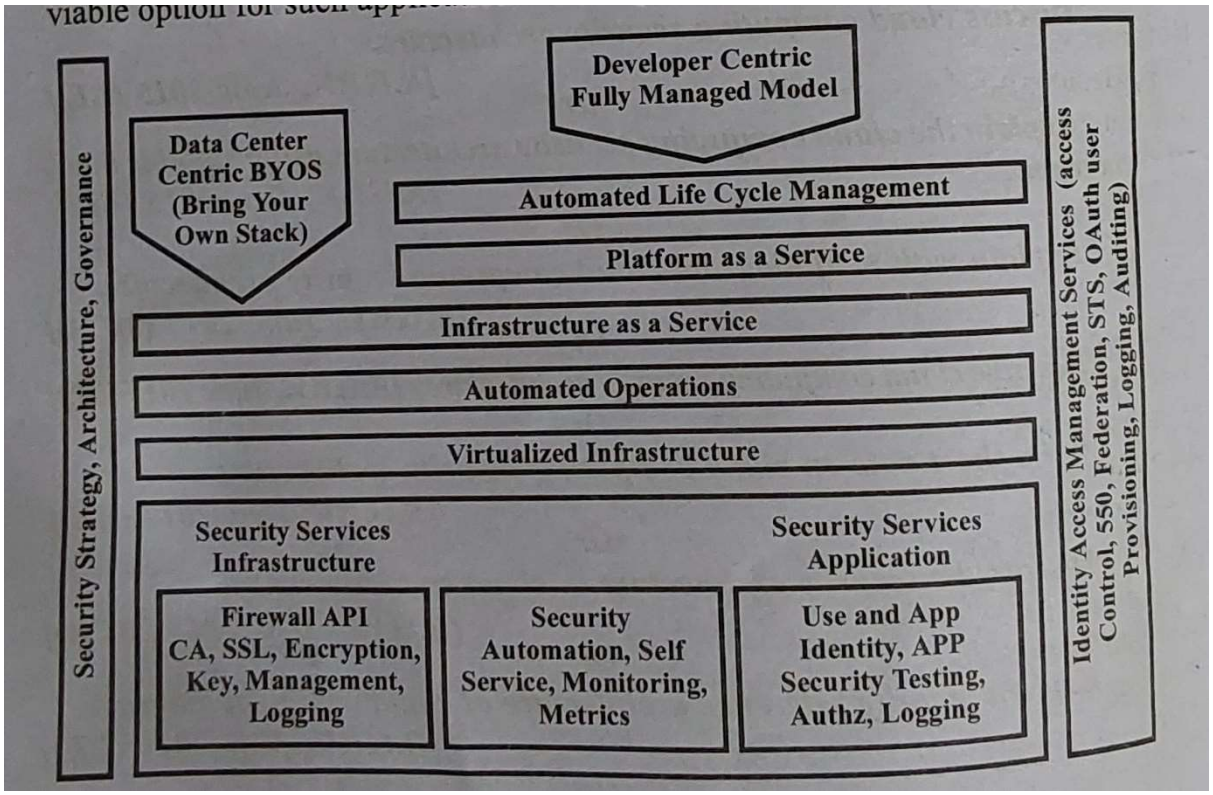
(iv) Other type designations include hybrid virtual machines and hardware-assisted techniques.

These classifications are somewhat ambiguous in the IT community at large. From a security perspective, there is a more significant impact when a host OS with user applications and interfaces is running outside of a VM at a level lower than the other VMs. Because of its architecture, the type 2 environment increases the potential risk of attacks against the host OS.

The Vmware infrastructure is managed by several users performing different roles. The roles assumed by administrators are the Virilization. Server Administrator Virtual Machine Administrator, and Guest Administrator. Vmware infrastructure users may have different roles and responsibilities, but some functional overlap may occur.

Cloud computing security architecture

Cloud application developer have been successfully developing application for IaaS and PaaS platform. These platforms offer basic security features but security concerns continue to be the number one barrier for enterprise cloud adoption. Cloud security concerns range form securely configuring virtual machine deployed on an IaaS platform to managing user privileged in a PaaS cloud. The cloud services can be delivered in many flavours, i.e in any combination of service delivery models SaaS, PaaS, and IaaS (SPI), and operational models, public, private, and hybrid, the cloud security concerns and solutions are context dependent. Hence the solution architecture should match these concerns and build security safeguards (controls) into the cloud application architecture



As a first step architects need to understand what security capabilities are offered by cloud platform. The architecture for building security into cloud service is shown in fig. Securely capabilities and offerings continue to evolve and vary between cloud provider. Hence you will often discover that security mechanism such as key management and data encryption service for encryption security artifacts and keys escrowed to a key management service. For such critical service, one will continue to rely on internal security services. A “Hybrid Cloud” deployment architecture pattern may be the only viable option for such application that dependent on internal services.

Principle component of cloud computing security architecture

User Layer Components –

(iv) Cloud applications
(ii) programming
(iii) Tools
(iv) Environments.

Service Provider Layer Components –

(iv) SLA monitor
(ii) Metering
(iii) Accounting
(iv) Resource provisioning
(v) Scheduler and dispatcher
(vi) Advance resource reservation monitor
(viii) Policy management.

Virtual Machine Layer Components –

(iv) Virtual machines
(ii) Operating systems
(iii) Monitoring of operating system.

Data Center Layer Components –

(iv) Servers
(ii) CPU's
(iii) Memory
(iv) Storage.

Question Bank

1. Explain cloud ecosystem

Or

Draw the diagram for cloud ecosystem

Or

Write short note on cloud ecosystem

2. Discuss cloud business process management (BPM). How cloud environment will help it

Or

Explain cloud business process management

3. Discuss cloud business process management with its life cycle

4. What is cloud analytics

5. How cloud analytics work

6. Define cloud security

7. Explain different cloud security services

Or

Discuss the different cloud security services

Or

Explain cloud security service

Or

Explain the categories of security service provided for information over the cloud

8. Write a brief note on cloud security design principle

Or

Discuss the various cloud security design principles

9. Discuss various type of security policy, and do you mean by term policy implementation

10. Explain the cloud computing security challenges

Or

List and explain various cloud computing security challenges

Or

List few cloud computing in security challenges

Or

Explain the cloud security challenges

Or

What are the different security challenges in cloud computing? Discuss each in brief

11. Explain virtualization security management

Or

Explain virtualization security management in cloud computing

Or

What do you understand by virtualization security management

Or

Write short note on virtualization security management

12. Discuss cloud computing security architecture

Or

Explain with diagram cloud computing security architecture

Or

Explain security reference architecture of cloud with neat diagram

Or

Explain security architecture design framework

13 Explain principal component of cloud computing security architecture

UNIT 5: Market Based Management of Clouds

Federated Clouds/Inter Cloud:
Characterization & Definition ,Cloud Federation Stack , Third Party Cloud Services . Overview of cloud applications:

ECG Analysis in the cloud, Protein structure prediction, Gene Expression Data Analysis ,Satellite Image Processing ,CRM and ERP ,Social networking .

Case study : Google App Engine, Microsoft Azure , Hadoop , Amazon , Aneka

- The notes have been prepared by using book mention in your syllabus i.e Mastering cloud computing by Buyya, selvi
- To get previous year question paper visit library
- The question that highlighted by yellow color, they should be your top priority for preparation
- As we move more further, I'll be updating the notes.

FAQs

Que: Do I have to use your notes for answer writing.

Ans:

- Nope the notes are prepared for students as for reference material, students who are too busy
- Yes, you can use these notes for answer writing.
- Or you can create your own notes or write answer in your word but it has to be specific
- Do not write YouTube answers or any website answer always follow university syllabus mention book for ref. so you can score more marks.

Architecture of cloud federation

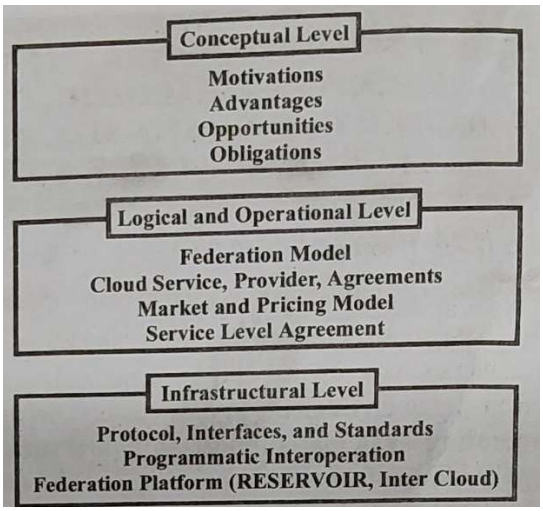
Or

3 different levels expressing the concept of inter cloud/cloud federation

Or

Cloud federation stack

Cloud federation includes research and development at the following levels - conceptual, logical and operational, and infrastructural. A complete view of the challenges faced to design and implement an organizational structure that coordinates together cloud services belonging to different administrative domains and make them operate within a context of a single unified service middleware is shown in fig. Each level introduces different challenges and works at a different layer of the IT stack. Then, it needs the utilization of different technologies and approach. Taken collectively, the solutions to the challenges faced at each of these levels form a reference model for cloud federation.



(i) **Conceptual Level** - This level addresses the challenges in presenting cloud federation as a favorable solution with respect to the use of services leased by single cloud providers. In this level, it is important to clearly identify the advantages of either service providers or service consumers in joining a federation and delineate the new opportunities that a federated environment creates with respect to the single provider solution.

(ii) **Logical and Operational Level** - This level addresses the challenges in devising a framework enabling the aggregation of providers belonging to different administrative domains within a context of a single overlay infrastructure, which is the cloud federation. Policies and rules for interoperation are defined at this level. Furthermore, this is the layer where decisions on how and when lo lease a service to - or to leverage a service from - another

provider are taken. The logical component defines a context within which agreements among different providers are settled and services are negotiated. The operational component characterized and shapes the dynamic behavior of the federation as a result of the choices of the single providers. Market oriented cloud computing is implemented and realized at this level.

(iii) **Infrastructural Level** - This level addresses the technical challenges involved in enabling heterogeneous cloud computing systems to interoperate seamlessly. It deals with the technology barriers that keep separate cloud computing systems belonging to different administrative domains By having standardized protocols and interfaces, these barriers can be overcome In other words, this level for federation is what the TCP/IP stack is for the Internet- a model and a reference implementation of the technologies enabling the interoperation of systems.

Benefits of federated cloud

The federation of cloud resources allows clients to optimize enterprise IT service delivery. The federation of cloud resources allows a client to choose the best cloud service provider, in terms of flexibility, cost and availability of services, to meet a particular business or technological need within their organization. Federation across different cloud resource pools allows applications to run in the most appropriate infrastructure environments. The federation of cloud resources also allows an enterprise to distribute workloads around the globe, move data between disparate networks and implement innovative security models for user access to cloud resources.

Intercloud architecture

The term intercloud is used interchangeably to express the concept of cloud federation. Intercloud expresses a composition of clouds that are interconnected using open standards to offer a universal environment for using cloud computing services. Intercloud represents a cloud of clouds and hence expresses the same concept of federating together clouds pertaining to different administrative organizations.

Intercloud Architecture - The intercloud architecture consists of two elements - cloud exchange and cloud coordinator. This is shown in fig.

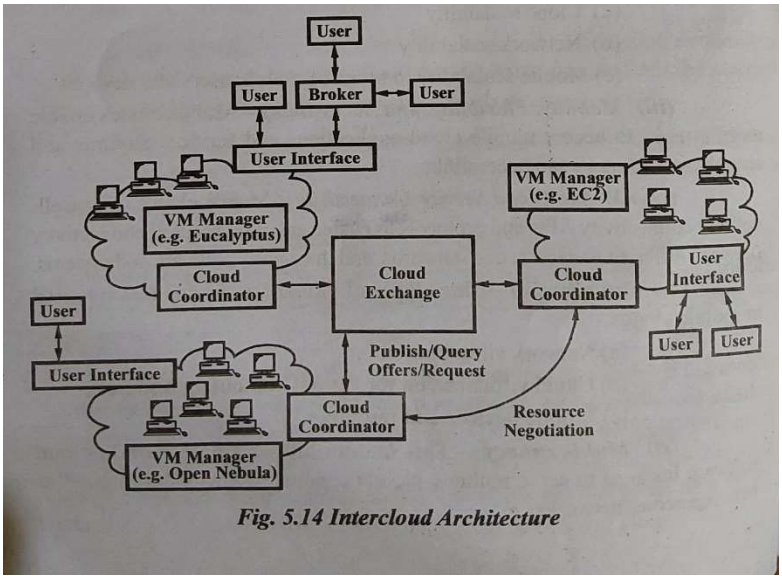


Fig. 5.14 Intercloud Architecture

(i) **Cloud Exchange**- It is the market-making component of the architecture. It provides services that permit providers to detect each other in order to directly trade cloud assets, as well as permits parties to register and execute auctions. In the second case, CloudExchange executes the auction. CloudExchange implements a web service based interface that permits data centers to join and leave the federation for providing such services to the federation

.(ii} **Cloud Coordinator** - It manages domain-specific issues pertaining to the federation. This is available on each party that wishes to join the federation. It contains front-end components and back-end components. The interaction of front-end components takes place with the CloudExchange and with other coordinators. The former permits data centers to mention their offers and needs, while the latter permits the coordinator to learn about the current state of the data center to determine whether actions from the federation are needed or not. Hence, when the coordinator finds that additional resources are needed by the data center, it initiates the discovery process of potential providers. As soon as the potential providers are found and the interested one is chosen, the coordinator meets the remote coordinator and communicates. Likewise, when CloudCoordinator finds that local resources are in use, they can mention an offer for resources in the CloudExchange, or they can search for matches among needs registered in the exchange service.

Other topic to be search : short notes question

- ECG Analysis in the cloud
- Protein Structure prediction
- Gene Expression Data Analysis
- Satellite Image processing
- CRM and ERP
- Social networking
- Aneka

Question Bank

1 Describe the architecture of cloud federation stack

Or

What are the three different levels expressing the concept of inter-cloud/cloud federation

Or

What do you mean by cloud federation stack

Or

Give a suitable definition of cloud federation stack and explain it in detail

Or

Write short note on cloud federation stack

2 Write benefits of cloud federation

3 What is intercloud? Explain architecture of intercloud

Or

Explain intercloud

Or

Write short note on intercloud

Google AppEngine

Google AppEngine is a Platform-as-a-Service implementation. It offers services for developing and hosting expandable Web applications. It is a distributed and scalable runtime environment that uses Google's distributed infrastructure to scale out applications handling several requests by allocating more computing resources to them and balancing the load among them. The completion of runtime is done by a collection of services permitting developers to design and implement applications that scale on AppEngine. The languages like Java, Python, and Go are used by developers, to develop applications. AppEngine constantly meters application's usage of Google resources and services. It bills users when their applications trespass free quotas.

Feature of Google AppEngine

Google application engine supports the following major features -

(i) Persistent storage, with query access sorting and transaction management features.
(ii) Scheduled tasks for triggering events at specified times or regular intervals.
(iii) Asynchronous task queues for performing work outside the scope of a request.
(iv) Automatic scaling and load balancing.
(v) One of either two runtime environments - Java or Python.
(vi) Authentication using Google Accounts API.
(vii) Dynamic Web services based on common standards.
(viii) A client-side development environment for simulating Google application engine on your local system.
(ix) Integration with other Google cloud services and APIs.

Google AppEngine with suitable block Schematic

Google AppEngine platform architecture are divided into four components -

(i) **Infrastructure** - Web applications can be hosted by AppEngine and its primary function is to serve users requests efficiently.

(ii) **Runtime Environment** -

(iii) **Storage** - There are three different level of storage - in memory cache, storage for semi-structured data and long-term storage for static data.

(a) Static File Servers - Web applications comprised of static and dynamic data. Static data is mostly constituted through the elements which express the graphical application layout (CSS files, sound files, java script files and plain html files) and data files. Dynamic data is a result of the application logic and the interaction with the user.

(b) Data Store - A service permitting developers to store semi-structured data is referred to the data store.

(iv) **Application Services** - Application hosted on AppEngine consider the most from the services made available by the runtime environment. These services simplify most of the common operations which are done in web applications.

(v) **Compute Services** –

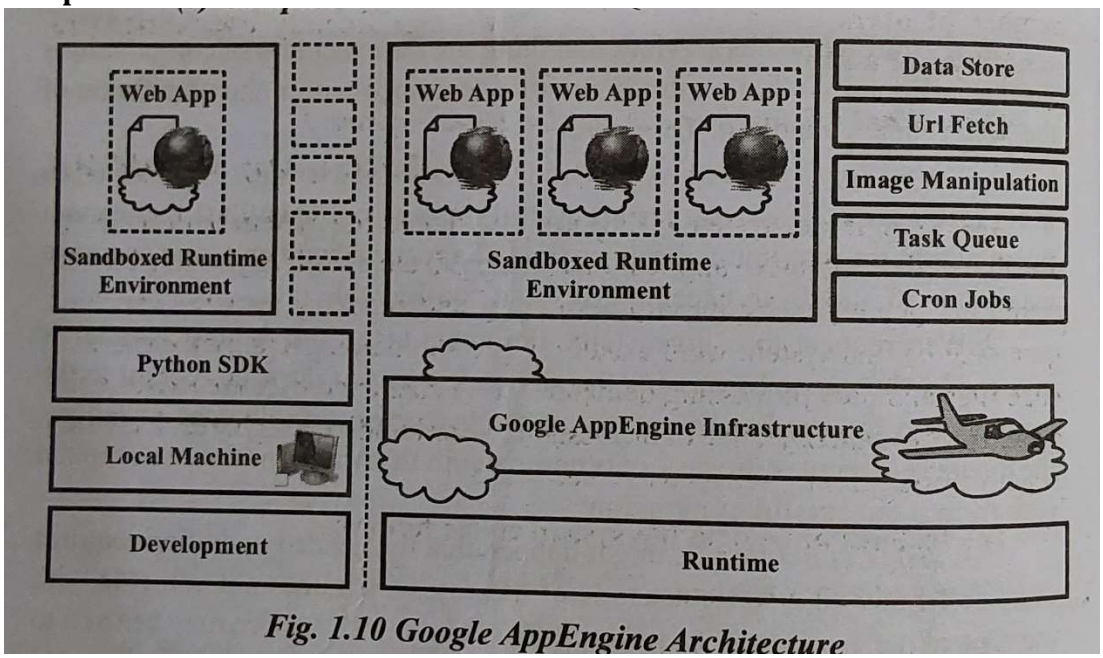


Fig. 1.10 Google AppEngine Architecture

Microsoft Azure

A Cloud operating system built on top of Microsoft data centers' infrastructure is Microsoft Windows Azure. Microsoft Windows Azure offers developers with a set of services for building application with the Cloud technology. The Azure platform can be used to scale any application that is built on the Microsoft technology. It integrates the scalability features into the common Microsoft technologies like SQL Server, Microsoft Windows Server 2008 and ASP.NET.

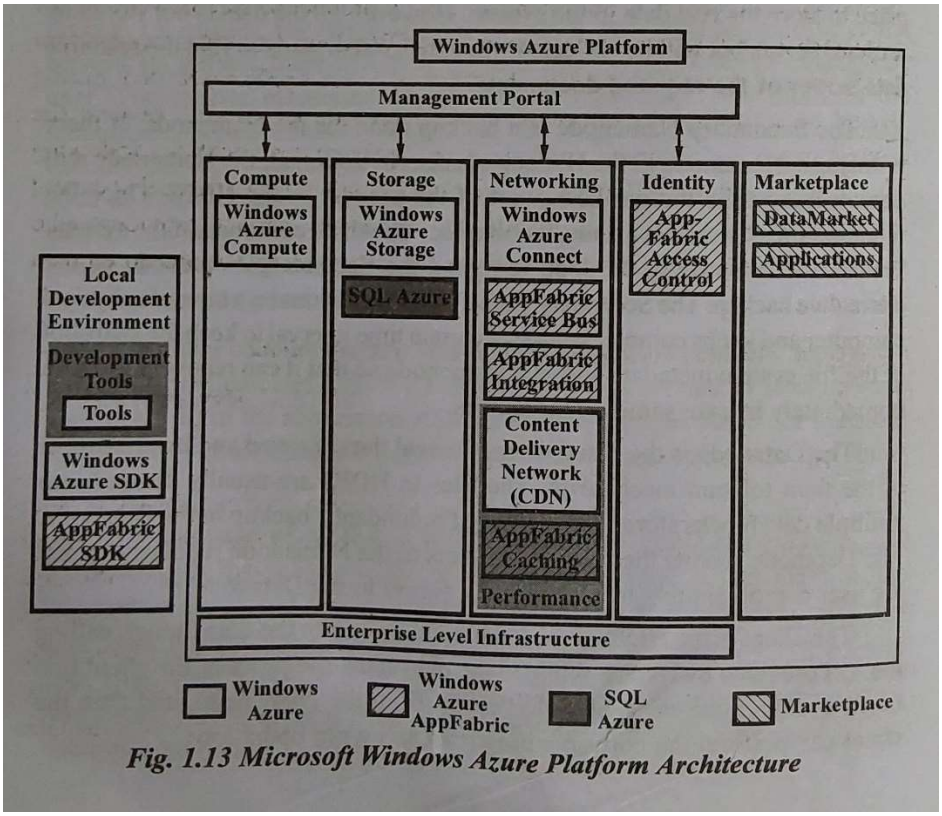


Fig. 1.13 Microsoft Windows Azure Platform Architecture

The services provided by Azure are shown in fig. The Windows Azure Management Portal manages and controls these services. It works as administrative console for all the services of the Azure platform.

Features of azure cloud platform

The features of Azure cloud platform are as follows -

(i) Microsofts Azure provides all three types of cloud computing i.e. SaaS, PaaS, and IaaS but major player in PaaS.

(ii) Microsoft Azure support hypersor based virilization based technology.

(iii) Two types of server support Azure such as linux and Window.

(iv) SQL Azure is a fully relational database support on Windows Azure.

(v) Windows Azure presently supports three roles - Web role, worker role, and VM role.

Services Provided by AWS

Amazon Web Services (AWS) is a platform that permits the development of flexible applications by offering solutions for elastic infrastructure scalability, messaging and file and data storage. The platform can be accessed through SOAP or RESTful web service interfaces and offers a Web based console where users can monitor and administrate the needed resources as well as their expenses computed on the basis of pay as you go.

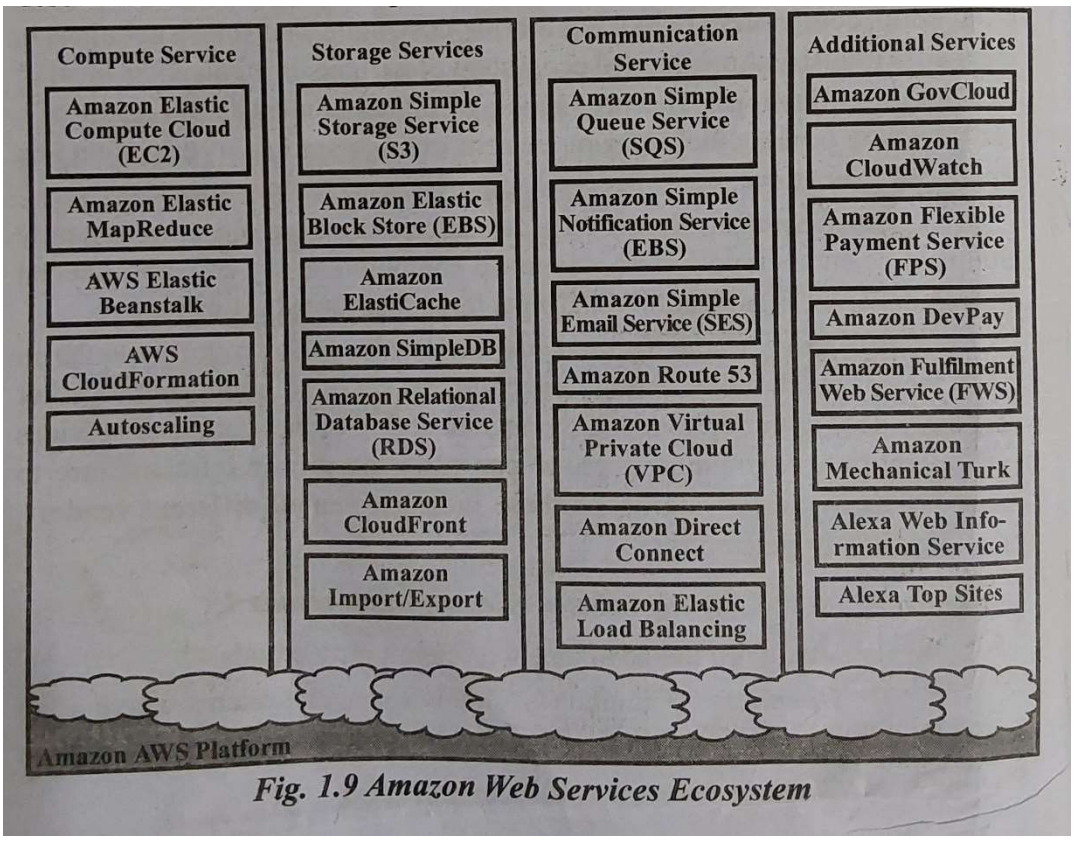


Fig. 1.9 Amazon Web Services Ecosystem

All the services available in the AWS ecosystem are depicted in the fig. There are services at the basis of the solution stack, which offer raw compute and raw storage-

Amazon Elastic Compute(EC2), and Amazon simple storage Service(S3). Elastic MapReduce and AutoScaling offer additional capabilities at the higher level for building smarter and elastic computing system. Solutions for reliable data snapshot and the management of structure and semi-structured data are offered by on the data side. Amazon Direct Connect cover the communication needs at the networking level. Amazon Simple Queue service (SQS), Amazon Simple Notification Service (SNS), and Amazon Simple mail Service (SES) are more advanced services for connecting applications. Other services are Amazon Cloudfront, Amazon Cloudwatch, Amazon Elastic BeanStalk, CloudFormation.

Storage services provided by Windows Azure

The different types of storage services provided by Windows Azure are as follows -

(i) **Blobs** - The large amount of data can be stored in the form of Binary Large Objects (BLOBs) using blobs service. For storing large text of binary files, this service is optimal. There are two types of blobs -

> (a)*Block Blobs* - Block blobs are made of blocks and they are optimized for sequential access and hence they are suitable for media streaming. Blocks are of 4 MB and the maximum dimension of a single block blob is 200 GB.
>
> (b) *Page Blobs* - Page blobs are composed of pages that are recognized by an offset from the starting of the blob. A page blob is divided into several pages or formed by a single page. A page blob is optimized for random access and used to host data distinct from streaming. A page blob can reach 1 TB of dimension.

(ii) **Azure Drive** - An entire file system can be stored in the form of a single virtual hard drive (VHD) file using page blobs. Then, a page blob can be mounted as a part of the NTFS file system by Azure compute resources, hence offering durable and persisting storage. Azure drive is a page blob mounted as part of an NTFS tree.

(iii) **Tables** - Tables form a semi-structured storage solution. They permit users to record information in the form of entities containing a collection of properties. Rows in the table represent the entities and are recognized by a key. These key forms the unique index built for the table. Users can insert, delete, update, and select a subset of the rows recorded in the table. There is no facility for representing relationships among entities and there is no schema enforcing constraints on the properties of entities. Due to this, tables are like spreadsheets instead of SQL tables.

The service handles huge amounts of data and query returning huge result sets. Two key characteristics offer in this sense - partial result sets and table partitions. A table can have maximum 100 TB of data and rows can contain maximum 255 properties with a maximum of 1 MB for each row. The maximum dimension is 1 KB for row keys and partition keys.

(iv) **Queues** - Applications can communicate by exchanging messages through durable queues, hence stopping messages from remaining unprocessed or getting lost. Messages are entered into a queue by applications. Other applications can read them in FIFO manner. When an application reads a message, the message is not marked as visible in order to make sure that messages get processed. After message processing, the application wants to explicitly delete it from the queue. This two-phase process makes sure that messages get processed before deleting them from the queue, and that client failures do not restrict messages from being processed.

Hadoop

Hadoop is an Apache-managed software framework created using MapReduce and Big Table. Hadoop allows applications based on MapReduce to run on large clusters of commodity hardware. The project has become the basis for the computing architecture underlying Yahoo!'s business. Hadoop is designed to parallelize data processing across computing nodes to speed computations and diminish latency. Two major components of Hadoop exist - a massively scalable distributed file system that can support petabytes of data, and a massively scalable MapReduce engine that computes results in batches.

Components of Hadoop - Two main components of Hadoop are as follows-

(i) **The Hadoop Distributed File System (HDFS)** - HDFS is the storage system for a cluster. When data lands in the cluster, HDFS breaks it into pieces and distribute those pieces among the different servers participating in the cluster. Each server stores just a small fragment of the complete data set and each piece of data is replicated on more than one server.

(ii) **MapReduce** - Because Hadoop stores the entire data set in small pieces across a number of servers, analytical jobs can be distributed in parallel to each of the servers storing part of the data. Each server evaluates the question against its local fragment simultaneously and reports its result back for collation into a comprehensive answer. MapReduce is the agent that distributes the work and collects the results. Both HDFS and Map Reduce are designed to continue to work even if there are failures. HDFS continuously monitors the data stored on the cluster. If a seiner becomes unavailable, a disk drive fails or data is damaged due to hardware or software problems, HDFS automatically restores the data from one of the known good replicas stored elsewhere on the cluster. MapReduce monitors the progress of each of the servers participating in the job, when an analysis job is running. If one of them is slow in returning an answer or fails before completing its work, MapReduce automatically starts another instance of the task on another server that has a copy of the data.

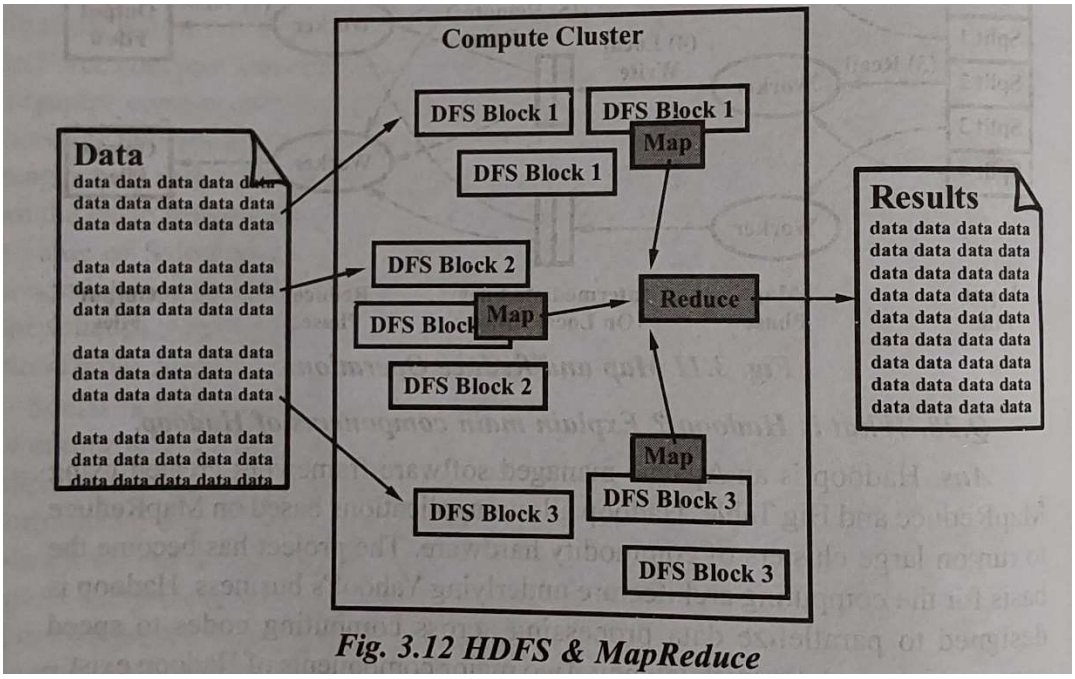


Fig. 3.12 HDFS & MapReduce

Because of the way that HDFS and MapReduce work, Hadoop provides scalable, reliable and fault-tolerant services for data storage and analysis at very low cost.

Architecture & Hadoop Advantage

Hadoop Architecture - Hadoop is an open-source framework that allows users to store and process big data in a distributed environment across clusters of computers using simple programming models. It is designed to scale up from single servers to thousands of machines with high degree of fault tolerance. Data in a Hadoop cluster is broken down into smaller pieces and distributed throughout the cluster like the Map and Reduce function that are executed on smaller subsets of larger data sets, and this provides the scalability needed for big data processing.

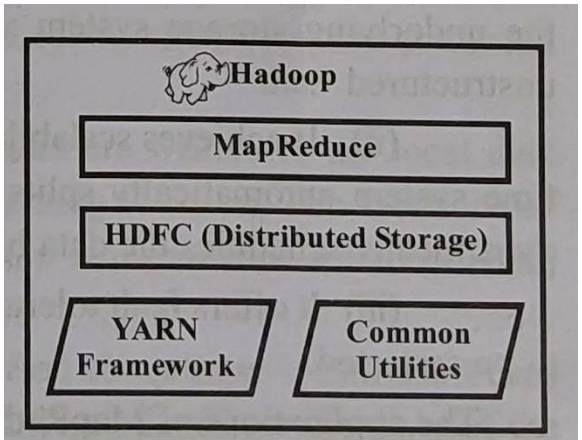


Fig. 3.14 Hadoop Architecture

Hadoop framework includes four models -

(i) **Hadoop Common** - They contain Java libraries and utilities that are required by other Hadoop modules. The Java libraries provide file system and OS level abstraction. It contains necessary Java files and scripts that are required to start Hadoop.

(ii) **Hadoop Yarn** - YARN is a cluster management technology. It is one of the key features in second-generation of Hadoop, designed from the experience gained from the first generation of Hadoop. YARN provides resource management and a central platform to deliver consistent operations, security and data governance tools across Hadoop clusters.

(iii) **HDFS (Hadoop Distributed File System)** - It is a distributed file system that provides high throughput computing access to application data.

(iv) **Hadoop MapReduce** - For large scale data processing this is programming model.

Advantages of Hadoop -

(i) The scalability and elasticity of free open source Hadoop running on standard hardware allow organizations to hold onto more data and take advantage of all their data to increase operational efficiency and gain competitive edge. Hadoop supports complex analyses across large collections of data at one tenth the cost of traditional solutions.

(ii) Hadoop handles a variety of workloads, including search, log processing, recommendations systems, data warehousing and video/image analysis.

(iii) Apache Hadoop is an open-source project by the Apache Software foundations. The software was originally developed by the world's largest Internet companies to capture and analyze the data that they generate. Unlike traditional, structured platforms Hadoop is able to store any kind of data in its native format and to perform a wide variety of analyses and transformation on that data. Hadoop stores terabytes and even petabytes of data inexpensively. It is robust and reliable and handles hardware and system failures automatically without losing data analyses.

(iv) Hadoop runs on clusters of commodity servers and each of those servers has local CPUs and disk storage that can be leveraged by the system.

Application of Hadoop

Now-a-days, with the rapid growth of the data volume, the storage and processing of Big Data has become the most pressing needs of the enterprises. Hadoop as the open source distributed computing platform has become a brilliant choice for the business. The users can develop their own distributed applications on Hadoop and processing Big Data even if they do not know the bottom-level details of the system. Due to the high performance of Hadoop, it has been widely used in many companies.

(i) **Hadoop in Yahoo!** - Yahoo! is the leader in Hadoop technology research and applications. It applies Hadoop on various products, which include the data analysis, content optimization, anti-spam e-mail system, and advertising optimization. Hadoop has also been fully used in user interests' prediction, searching ranking, and advertising location.

In the Yahoo! home page personalization, the real-time service system will read the data from the database to the interest mapping through the Apache. Every 5 minutes, the system will rearrange the contents based on Hadoop cluster and update the contents every 7 minutes.

Concerning spam e-mails, Yahoo! uses the Hadoop cluster to score the e-mails. Every couple of hours, the Yahoo! will improve the anti-spam e-mail model in the Hadoop clusters and the clusters will push 5 billion times of e- mails' delivery every day At present, the largest application of the Hadoop is the Search Webmap of Yahoo!, it has been run on more than 10000 Linux cluster machines.

(ii) **Hadoop in Facebook** - It is known that Facebook is the largest social network in the world. From 2004 to 2009, Facebook has over 800 million active users. The data created everyday is huge. This means that Facebook is facing the problem with big data processing which contains content maintenance, photos sharing, comments, and users access histories. These data are not easy to process so Facebook has adopted the Hadoop and Hbase to handle it.

Question Bank

1 What is Google AppEngine

Or

Write short note on Google AppEngine

2 Describe major cloud feature of Google application engine

Or

List the major features of Google App Engine

Or

Explain the major cloud feature of Google application engine

3 Explain the user view of Google AppEngine with suitable block schematic

4. Write short note on Microsoft Azure

Or

Discuss about Microsoft Azure case study

Or

Write short note on Azure

5. Discuss the storage services provided by window azure

Or

Illustrate the services that are provided by window azure operating system

6. What is AWS? What types of services does it provide

7. Explain the services provide by the amazon infrastructure cloud from a user perspective

Or

Describe the services offered by AWS

8. What is Hadoop? Explain main component of Hadoop

9. Explain the application of Hadoop

10. What are the advantage of Hadoop? Explain Hadoop architecture with proper diagram