CLOUD COMPUTING.
CS 468-A.

(7) (a). Secure Software Development Life Cycle (Sec SDLC)

(*) The Sec SDLC involves identifying specific threats and thee risks they represent, followed by design. and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and its customer.

(*) The SDLC consists of 6 phase and there are steps unique to the Sec SDLC in each of the phases:

→ Phase 1 : Investigation → Define project processes and goals, and document them in the program security policy.

→ Phase 2 : Analysis → Analyze existing security policies and pgms, analyze current threats and controls, examine legal issues and perform risk analysis.

→ Phase 3 : Logical design → Develop a security blueprint, plan incident response actions, plan business responses to disasters. and determine the feasibility of continuing or outsourcing the project.

→ Phase 4 : Physical design → Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions and review and approve plans.

→ Phase 5 : Implementation → Buy or develop security solns. At the end of this phase, present a tested package to management for approval.

→ Phase 6 : Maintenance → Constantly monitor, test, modify, update and repair to respond to changing threats.

clarify

(7) (b) Data Governance Framework.

The major 5 components of data governance framework are :

Phase 1 : Understanding the problem.
    Inorder to maximize the efficiency, it is important to talk to the executives and managers across the organization and understanding what main point they would like to solve.

Phase 2 : Strategizing and Planning.
    During this phase, we outline both strategic and tactical approaches focussed on achieving the long term goals.

Phase 3 : Organizing
    After discussing and choosing a correct plan, we also need to gather all the information together so we will require a data governance council to organize all the information.

Phase 4 : Communicating.
    Data Governance program extend over a period of time and program fatigue can be common. Good communications lead to continued by in from the pgm sponsors.

Phase 5 : Executing
    After gathering all the data, organizing it and developing plan, the final phase is to execute the plan.

8 (a) cloud services used in online calendar Application
→ Most computers users today have embraced keeping their schedules on their PC.
→ But the problem of such type of calendar software is that all the appointments and meetings have to reside on a single computer.

→ We won't be able to access the schedule if our PC is not nearby.

→ So instead of using a calendar that's wedded to a single computer, many users are moving to web-based calendars..

→ A web based calendar service stores your calendar on the Internet, where they can be accessed from any computer that has an Internet connection.

→ Web based calendars are also extremely easy to share with others users in any location, which make them great for collaborative projects.

Google calendar.

→ The most popular web-based calendar today no doubt due to its association with the web's most used search engine is a google calendar.

→ Google calendar is free, full featured and easy to use.

→ It lets you to create both personal and shared calendars, which makes it ideal for tracking business group, family & community schedules.

→ There are different variety of calendars:

✱ Personal calendar : (Default calendar).

   (i) Like all web based calendars all the events are stored in the cloud.

   (ii) It means that you can access your calendar from any device via the web.

✱ Public calendar, which others can access via the web.

   (i) creating a public calendar and all employees or attendees can access it via the web.

✱ Holiday calendars, which add national / international occations, holidays or festival to a basic calendar.

→ You can create one calendar for home, another for work. Then you can view your calendars from the same Google calendar page, with the events from each calendar color coded for easy visibility.

→ Google Calendar can scan the your email messages for dates and times and with a few clicks of your mouse, create content based on your Gmail messages.

⑧ (b) Security challenges

→ Physical Security — In cloud, you cannot provide physical security.

→ Shared Resource — In cloud (public) you are sharing resources
 — when in a shared environment you don't have any knowledge or control of where the resources run.

→ Vendor Lock -in — is another challenge.
 — when choosing cloud-based services, its important to check to see how easy it would be to migrate from that service to another.

→ Integrity of data. — Data integrity means ensuring the data is identically maintained during any operations

— — Ensuring the integrity of the data really means that it changed only in response to authorized transactions.

→ Data Compliance — The data owner is still fully responsible for compilance.

→ Access to Log — Security managers need to make sure to negoti negotiate access to the provider logs as part of any service management.

⑤ ⓐ. **MapReduce**

→ A software framework which supports parallel and distributed computing on large data sets.

→ MapReduce s/w framework provides an abstraction layer with the data flow and flows of the controls of users & hides the implementation of all data flows steps such as data mapping.

Intermediate key pairs.
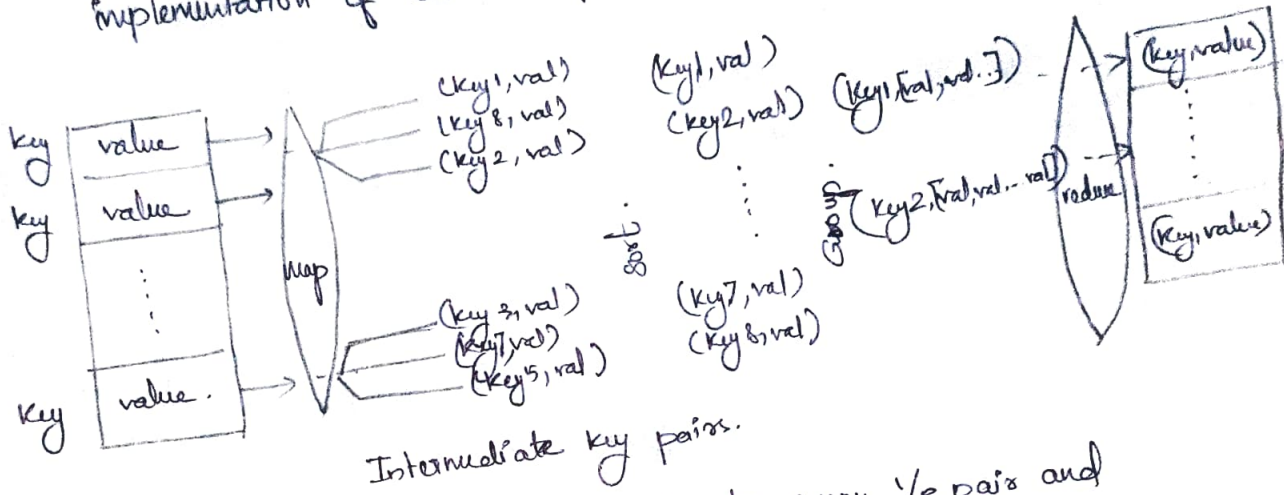
The Map func is applied in parallel to every I/p pair and produce new set of intermediate (key value) pairs as follows:

$$(key1, val1) \xrightarrow[func]{map} Lists (key2, val2).$$

Then the MapReduce library collects all the produced intermediate pairs from all I/p pairs & sort them based on the 'key part. Finally the Reduce func. is applied in parallel to each grp. producing the collection of values as o/p as illustrated here. at

$$(key2, List(val2)) \xrightarrow{R.f} List (val2)$$

⑤ ⓑ   **Map Reduce**

Ⓐ Distributed search
Ⓑ Calculation of pairwise.
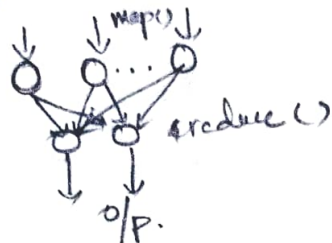Ⓒ distance of sequence (BLAST).

Iterative Map Reduce.

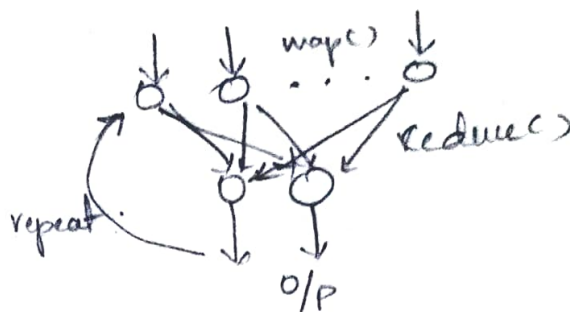Ⓐ Data mining including
  - clustering
  - k means
  - MDS.

6.

Map Reduce	Iterative Map Reduce
① Distributed sort	① Linear Algebra.
② High energy physics (HEP) histograms.	② Expectation & max^m algorithm.
③ Information retrieval	

① (b) <u>Memory Virtualization</u>

② Virtual memory virtualization involves sharing the physical system memory in RAM and dynamically allocating it to the physical memory of the VMs.

② Two-stage mapping process should be mainted by the guest OS and the VMM, respectively: virtual memory to physical memory and physical memory to machine memory.

③ Mapping of virtual addresses to the physical memory addresses of VMs ⟶ Guest os.

④ Guest os cannot directly access the actual machine memory.

⑤ Guest physical memory to actual machine memory ⟶ VMM.

⑥ Each page table of the guest OSes has a separate pg. table in the VMM corresponding to it, called the shadow pg. table.

⑦ Physical memory addresses are translated to machine addresses using another set of pg tables defined by the hypervisor.

⑧ VM ware uses shadow pg tables to perform virtual-memory-to-machine-memory address translation.

② ⓐ Platform-as-a-Service (Paas)

⊕ This model provides users with a cloud environment in which they can develop, manage and deliver applications.

⊕ Platform includes OS and runtime library support.

⊕ An integrated ~~of~~ computer system consisting both h/w & s/w infrastructure.

⊕ the user does not manage the underlying cloud infrastructure.

⊕ Enables a collaborated s/w development platform for users from diff parts of the world.

⊕ Provides manage security, OS, ~~st~~ server s/w and backups.

⊕ Facilitates collaborative work even if teams work remotely.

⊕ Paas provides a platform with tools to test, develop & host applications in the same environment.

② ⓑ ① Public cloud

⊕ A public cloud is built over the internet and can be accessed by any user who has paid for the service.

⊕ Public cloud delivers a selected set of business processes.

⊕ the application and infrastructure services are offered on a flexible price-per user basis.

eg: Google App Engine (GAE), AWS.

① Private cloud.

⊕ A private cloud is built within the domain of an intranet owned by a single organization.

⊕ Client owned and managed and access is limited to the owning clients and their partners.

eg: a company have their own domain is an example of private cloud.

(iii) Hybrid cloud.

* A hybrid cloud is built with both public and private clouds.
* Private clouds can also support a hybrid cloud model by supplementing local infrastructure with computing capacity from an external public cloud.
* The RC2 is a private cloud built by IBM that interconnects the computing and IT resources at 8 IBM Research centers scattered throughout the world.
* A hybrid cloud provides access to clients, the partner n/w and third parties.

④ ⓐ There a 3 static cloud resource provisioning policies.

ⓐ over provisioning with the peak load causes heavy resource waste

ⓑ underprovisioning with the peak of resources result in losses by both the user and provider in that paid demand by the users is not served and wasted resources still exist for those demanded areas below the provisioned capacity.

ⓒ the constant provisioning of resource with fixed capacity to a declining user demand could result in even worse resource waste.

(a).

(b).
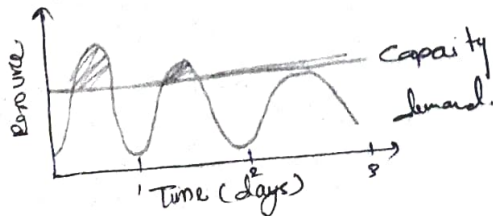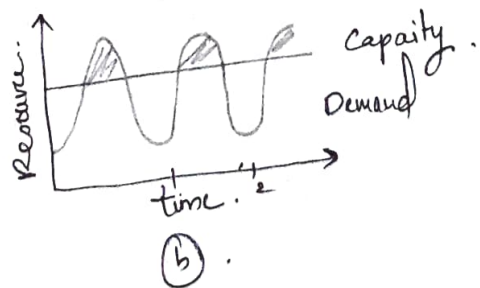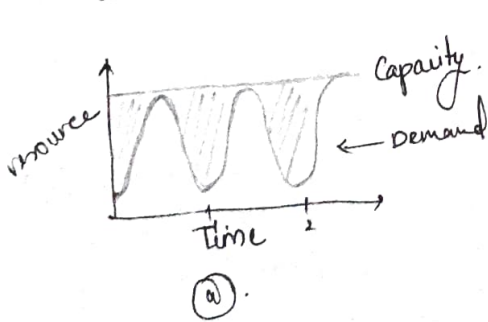
① ~~Virtualism~~

ⓐ ① <u>Instruction set Architecture Level</u>

⊛ Virtualization is performed by emulating a given ISA by the ISA of the host machine.

⊛ eg: MIPS binary code can run on an x86 - based host machine.

⊛ Legacy binary code is written for various processors can be run on any given new h/w host machine.

⑪ <u>Hardware Abstraction Level</u>

⊛ Performed right on top of the bare h/w, generates a virtual h/w environment for a VM.

⊛ Also manages the underlying h/w through virtualization.

eg: IBM VM/370.

⑫ <u>Operating System Level</u>

⊛ Abstraction layer b/w traditional os and user application

⊛ the containers behave like real servers.

⊛ commonly used in creating virtual hosting env. to allocate h/w resource among a large no. of mutually distributing users.

⑭ <u>Library Support Level</u>

⊛ Most application uses API exported by user level libraries lengthy system calls by the os.

⊛ Virtualization with library interfaces is possible by controlling the communication link b/w app. and the rest of a system through API hook.

⊛ eg: v CUDA.

Ⓥ Ⓤser Application Level

① Most popular approach is to deploy high level lang. VMs.

② Any pgm written in the HLL and compiled for this VM will be able to run on it.

eq: Microsoft .NET CLR & JVM.

④ ⑥. V.M Creation & Management

cloud loading experiments are used by Melbourne research group on the French Grid 5000 systems. this exp. setting illustrates VM creation and management.

the manager provide a public API for users to submit and control the VM.

the VM manager is the link b/w the gateway and resources. the manager manages VMs deployed on a set of physical resources.