MST-2

CLOUD QUESTION BANK-

2 Mark Questions

Ques1:- Define the terms backup and recovery. Discuss.

Ans:- **backup:-** A backup or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original data after a data loss event.
Cloud backup is a service in which data and applications on a business's server are backed up and stored on a remote server.
Business's opt to back up to the cloud to keep files and data readily available in event of system failure, outage or natural disaster.

Recovery:- Data recovery is process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible.
Cloud disaster recovery is a service that enables backup & recovery of remote machines on a cloud-based platform.
Cloud disaster recovery is primarily an IaaS solution that backs up designated system data on a remote offsite cloud server.

Ques2:- What do you mean by monitoring and management of cloud security?

Ans:- (a) **Cloud security Monitoring :-** * [also study benefits of cloud security Monitoring]
It is an essential aspect of cloud management & security.
[ ] supervising servers, both virtual & physical, in order to continuously assess and analyze data and infrastructure for threats & vulnerabilities.
Cloud security Monitoring solutions rely on automation features in order to provides on going support & assessment capabilities that reduce risk of costly data breaches.
Depending on a company's hosting platform, some cloud security monitoring is built into application & server hosting, while others are externally added to an existing infrastructure.

(b) Cloud Security Management :-
Security Management in cloud is set of strategies designed to allow a business to use cloud applications & networks to their greatest potential while limiting potential threats & vulnerabilities. This is done with tactics : identifying & assessing cloud services.

Ques3:- Define with examples:- troubleshooting & maintainance in cloud management.

Ans:- (a) Troubleshooting :- It is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and explain how to resolve the problem. For example, when a laptop won't boot up, an obvious first step is to check whether power cable is working. once common issues are ruled out, troubleshooters must run through a checklist of components to identify where failure is happening.

(b) Maintenance in cloud :-
Cloud-based computerized maintenance management systems (CMMS) can be assessed by web browser or app. This means that maintenance staff can retrieve relevant information wherever they are located. Maintenance can be planned, scheduled, monitored & automated from a web browser.

Ques4:- What do you mean by service level agreement in cloud management?
Ans:- A service ~~for~~ level agreement (SLA) is the bond for performance negotiated ~~by~~ cloud services provider & client.
Service level agreements are standardized until a client becomes large consumer of cloud services.
Service level agreements are defined at different levels mentioned below:-

SDN → ① Traditional networking (source to destination package sent via router)

(a) Customer - Based SLA
(b) Service Based SLA
(c) Multilevel SLA

Few service level agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating level Agreement (OLA) & may not have restriction of law.

SLA specify some parameters :-
① Availability of service
② Latency or response time
③ service components reliability
④ Each part accountability
⑤ Warranties.

A centralised structure for the network that can communicate & command rest of network.

design
↑ the software
SDN - SOFTWARE DEFINED NETWORK

4 MARKS QUESTIONS

makes processing fast with SDN controller by keeping check on entire network

Ques5:- Discuss in detail the following real world statement, "Software defined networking is used with open stack gives most valuable result", support this statement with diagram.

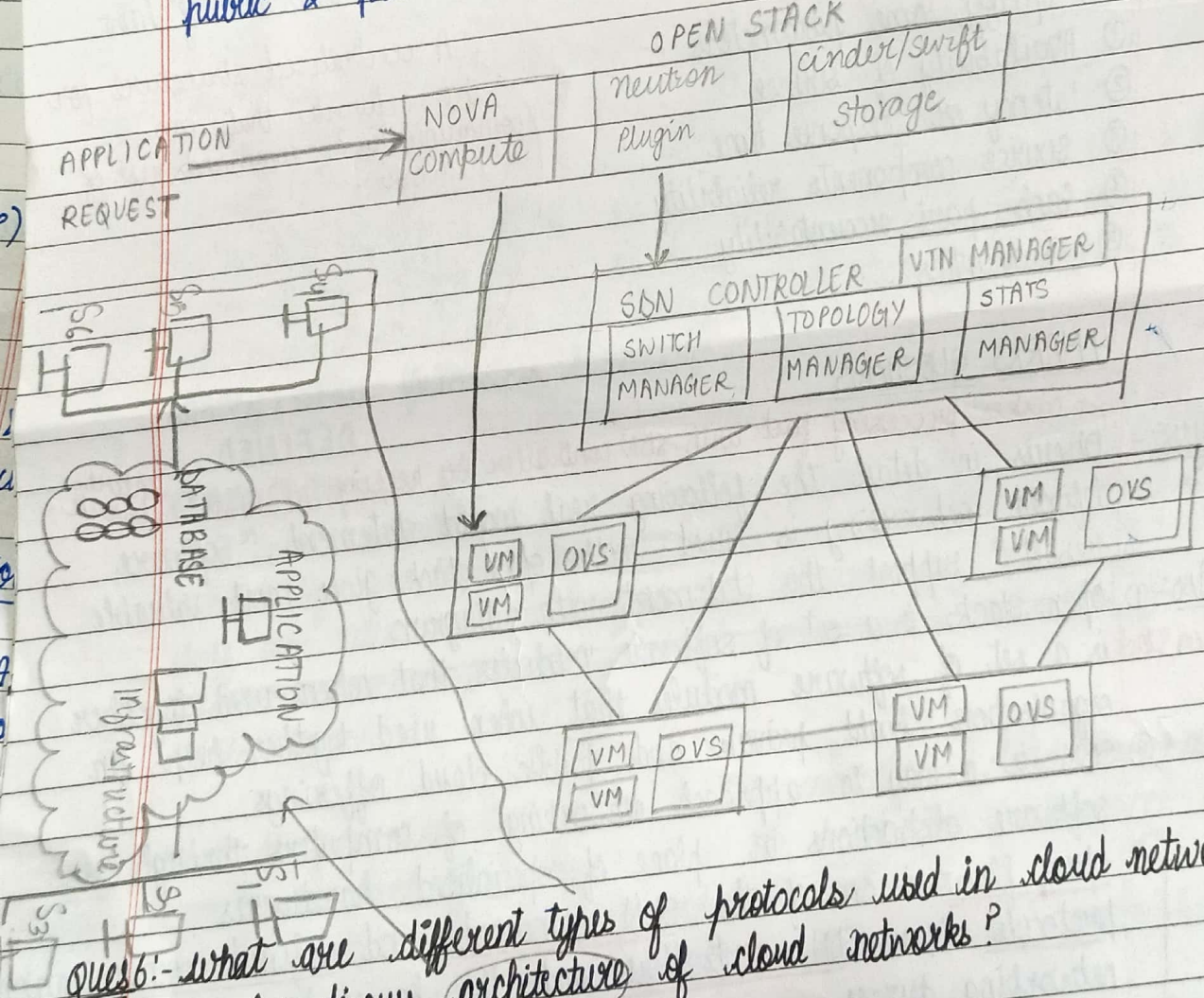
Ans:- ① Open Stack is a set of software modules that when used together
Open Stack is a set of software modules that when used together helps an organisation build private and public cloud offerings.

② SDN is a way to approach networking of computers through software abstractions in place of specialised hardwares.

③ Open flow is one of the SDN standards and defined communication protocols b/w SDN controllers and the forwarding plane of networking devices.
Its benefits includes programmability, centralized intelligence & how it abstracts network architecture.

SDN comprises of 3 layers → ① Application Layer
② Control Layer
③ Forwarding / Infrastructural layer.

④ SDN is an emerging approach to handle data forwarding and control seperately. Its implementation strategy relies on open source.
⑤ By providing practical management tools and abstractions that hide underlying physical network's complexity, SDN allows operators to build complex, networking capabilities on demand.
Open stack is an open source cloud platform that helps build public & private cloud at scale.



Ques 6:- what are different types of protocols used in cloud networks and also discuss architecture of cloud networks?

* Architecture of Cloud

Protocol is a set of rules that allow 2 electronics item to connect and exchange information to one another.

Date
Page

~~Architecture of Cloud~~

Network protocols are set of rules, conventions, data structures that dictate how devices exchange data across networks.

Cloud IOT core supports two protocols for device connection and communication : MQTT and HTTP.

Names → Types :-
① Gossip Protocol :- communication protocol, used for failure detection, monitoring & messaging
② Connectionless Protocol :- carries mechanism of fragmentation.
③ State Routing Protocol :- It is used to know the information about path / routing.
④ Internet Group Management Protocol :- Its communication protocol used to multicast the data to nodes via router.
⑤ Secure Shell protocol :- allows remote login securely over internet

same Ans 13

Types → ① Network Management
② Network communication
③ Network security.

Architecture

Businesses can evaluate three different cloud network architecture deployment methods.

① Built-in networking tools :- The first method is to simply use CSP's built-in networking tools provided as part of base of IaaS. Using it means, one needs to configure and manage IaaS cloud independently of any other private or public cloud.
② Virtual networking appliances :- The second method is to use virtual networking appliances from networking vendor to handle networking tasks, instead of built-in tools offered by cloud provider.
③ Multi-Cloud Management platform :- These are to create a software overlay between private and public clouds, which masks underlying differences in configuration management.

NFV → creates virtualization classes of network node functions & link building blocks to allow diff. network services

NFV → way to virtualize network services like router, load balancer, firewalls

Ques 7:- Draw a diagram with example/s and discuss real world case where Network functions visualisation is utilized?

Ans:- NFV - Network function virtualisation is technology that virtualizes full classes of network node functions & creates building blocks that link together to allow different networking services.

→ NFV allows enterprises to design, provide, & ease into much more advanced services & operations, as well as reduce outgoings through cost savings.

→ It runs software defined network functions which are independent of hardware platforms.

There are various cases in which NFVs are being used like :-

① Network Virtualisation

Reduce hardware

Network Virtualisation gives service providers the agility & flexibility they need when rolling out new network services. It helps them reduce their spending on bulky physical hardware & costs associated with running, maintaining & occassionally repairing it. One of best examples of network virtualization is new MEC & SD-WAN

② Mobile Edge Computing

translates various components of mobile like radio towers / data centres from hardware to software

using NFV allows edge computing devices to perform computational services & provide network functions by generating & utilising either single or multiple virtual Machines.

Multi Access Edge Computing (MEC) is clear example of it. It is utilising mobile edge computing to provide ultra low latencies.

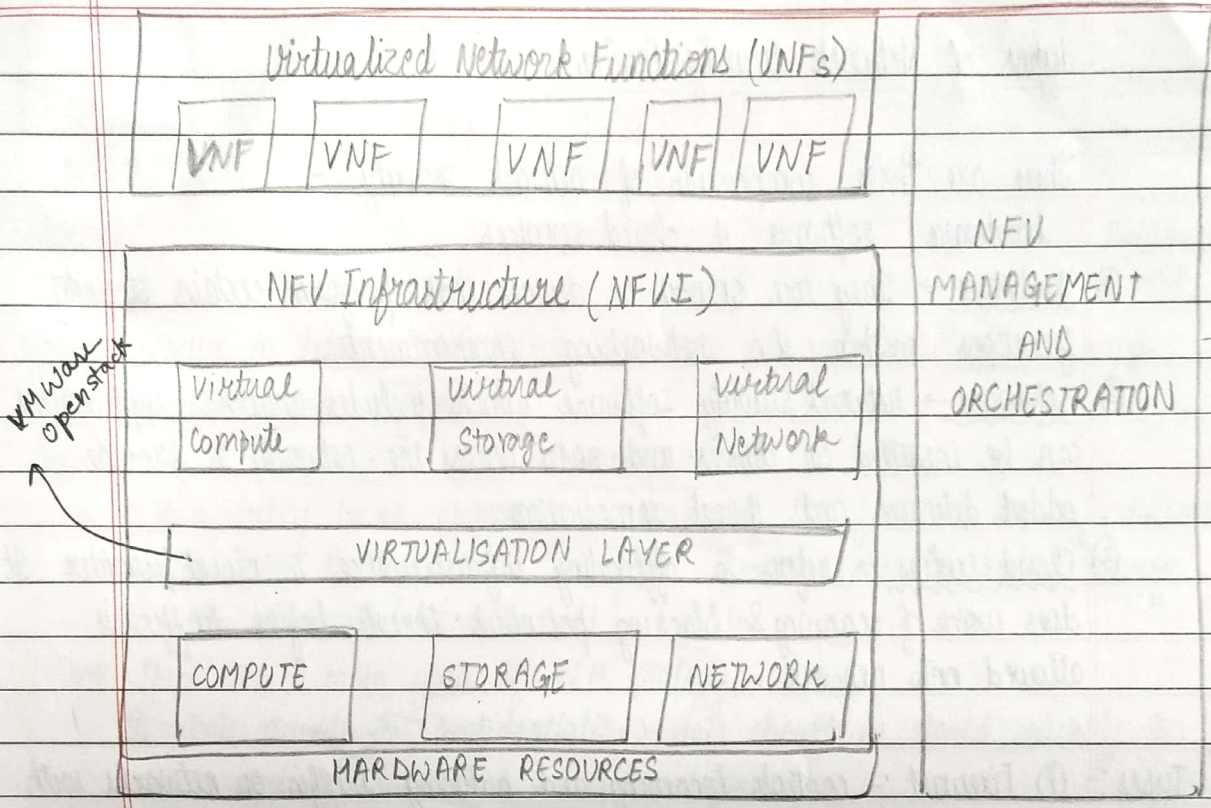
③ Orchestration Engines → uses programming to manage connections b/w network function services

④ Video Analytics → reduces bandwidth upto 90% → camera or IOT devices

⑤ Security → Firewalls protect VMs

⑥ Network Slicing → slice physical networks to multiple networks

NFV uses virtualization and aims to support infrastructure totally independent of hardware.



Ques8:- "Whenever any cyber attack takes place, cloud system is ready to manage" - To support this statement provide role of security & how cloud security is going to help by discussing the types of network security & their level of usage with diagram.

Ans:- Cloud security is a collection of security measures designed to protect cloud-based infrastructure, applications & data. These measures ensure user & device authentication, data and resource access control and data privacy protection.
There are various roles which provide clarity on how industry trends are affecting security professionals:-

1) Security leadership
2) security architect
3) Security posture & compliance
4) Platform security engineer
5) Application security engineer

ayers of Network security:- ① Prevention
② Detection
③ Response.

Date
Page

Types of Network Security Devices

There are three components of network security :-
hardware, software & cloud services.

① Hardware → They are servers or devices that perform certain security functions within the networking environment.

② Software → Network security software which includes antivirus applications, can be installed on devices and nodes across the network to provide added detection and threat remediation.

③ Cloud services → refers to offloading infrastructure to cloud provider. It does work of scanning & blocking potential threats before traffic is allowed onto network.

Types :- ① Firewall :- controls incoming and outgoing traffic on networks with pre-determined security rules.

② Network Segmentation :- defines boundaries between network segments where assets within group have common functions, risks or role within an organisation.

③ Access Control :- It defines the people or threats groups & devices that have access to network applications & systems, denying unsanctioned access, & maybe threats.

④ Remote Access VPN :- provides remote & secure access to a company network to individual hosts or clients.

⑤ Zero Trust Network Access → permits access to ~~target network~~ organisation's applications from users who require that access to perform their duties.

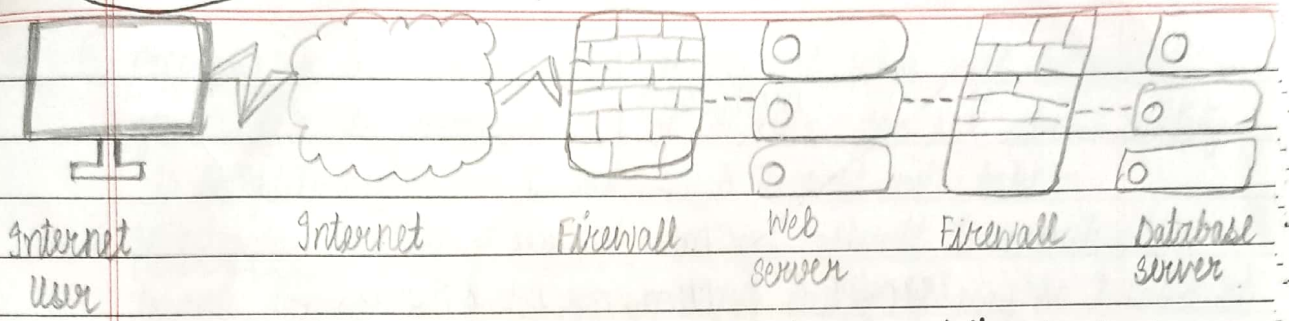
⑥ EMail Security → refers to processes, products & services designed to protect your email accounts & mail content safe from external threats.

⑦ Data loss Prevention → cybersecurity methodology that combines technology & best practices to prevent exposure of sensitive information.

security integrity availability

GSUAD — DATA

generate store use | destroy archive



Ques 9→ Discuss in detail about "Data life Cycle Management" with proper diagram and example.

Ans:- DATA LIFE CYCLE MANAGEMENT

→ DLM is policy based approach to managing the flow of an information's system data throughout its lifecycle: from creation & initial storage to when it becomes obsolete and is deleted.

→ There are 3 main goals of DLM strategy:-

ⓐ Data security & confidentiality:- data should be stored securely to ensure private, confidential & sensitive information.

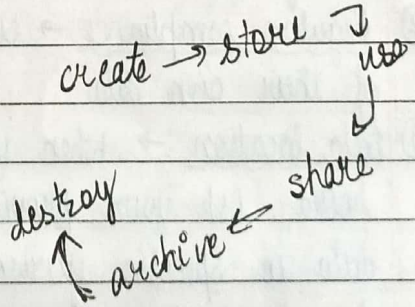
ⓑ Data integrity:- data must be accurately stored.

ⓒ Data availability:- Approved users should be able to access the data, when & where they need access without disruptions.

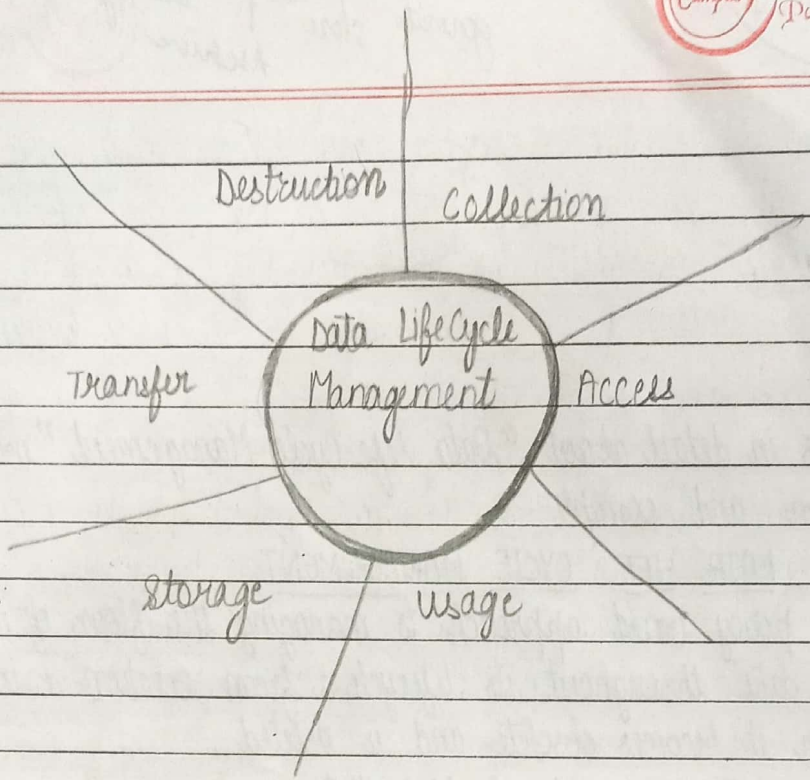
→ Data Management experts stress that DLCM is not a product, but a comprehensive approach to manage an organisation's data, involving procedures & practise as well as applications.

→ There are 5 phases of DLCM:-

① Generate And Collect Data
② Store And Manage Data
③ Use And Share Data
④ Archive data
⑤ Destroy data



→ For eg, an administrator can use a DLM product to search stored data for a certain file type of a certain age.



Question → what are Gartner's seven cloud computing security risks?

Ans:-

The following are security risks, Gartner says that customers should raise with vendors before selecting a cloud vendor.

① Privileged user Access → Sensitive data brings inherent level of risk. So get as much information as you can about the people who manage your data.

② Regular compliance → customers are responsible for security & integrity of their own data.

③ Data location → When you use cloud, you won't know where data is hosted. Ask your providers if they commit to storing & processing data in specific jurisdictions, & whether they make commitment to obey local privacy requirements.

④ Data segregation → encryption is effective, but isn't cure. One needs to find out what is done to segregate data at rest.

→ restoration of data.

⑤ Recovery → A cloud provider should tell what will happen to your data & service in case of disaster. Also ask about ability to complete restoration & how much time it will take.

⑥ Investigative support → Cloud services are difficult to investigate, because logging & data for multiple customers may be located at & spread across ever changing set of locations.

⑦ Long Term Viability → Ask potential providers how would you get your data back & if it would be in a format that one could import into replacement application. (Cloud provider would never go broke or get acquired & swallowed up by a large company).

Ques II → Why open stack security is necessary & discuss about RBAC – Role based Access control ?

Ans:- Open Stack is an open source platform that uses pooled virtual resources to build and manage public & private clouds.
It provides security groups for both hosts and network to add defense in depth to virtual machines in a given project.

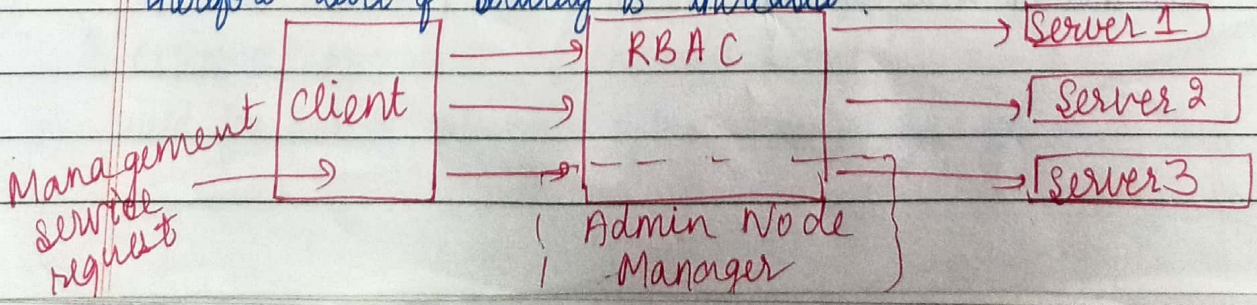
* It is an important part of cloud since it provides common, open standard through its API & allows portability b/w cloud environments.

need → ① open source ② anyone track open softwares ③ flaws easily detected ④ common vulnerabilities & exposure can be found.

Role Based Access Control

limited access is provided and also with permission

1. It is a mechanism that restricts system access. It involves setting permissions & privileges to enable access to authorized users.
2. Its concept is to create a set of permissions & assign these permissions to user or group.
3. With help of these permissions, only limited access is provided therefore level of security is increased.



MUI MAIHLE
MAIHLE

Misconfiguration
Unauthorised Access
Insecure APIs
Hijacking of accounts
Lack of visibility
External sharing of

Campus
Date
Page

Ques12 → "IT industries nowadays have a lot of threats on cloud" - discuss whether it is true or false by supporting your answer with real world example & also tell what are new threats to cloud services now-a-days?

Ans:- There are various threats to cloud services :-

① Misconfiguration :- Many organisations are unfamiliar with securing cloud infrastructure & often have multi-cloud deployments, it is easy for misconfiguration or security oversight to leave an organisation's cloud based resources exposed to attackers.

② Unauthorized Access :- While this is an ~~access~~ asset (accessible from public network), it makes easier for an attacker to gain access to an organisations cloud based resources.

③ Insecure Interfaces / APIs :- It creates potential issues if customer has not properly secured the interfaces for their cloud based infrastructure.

④ Hijacking of Accounts :- Many people have extremely weak password security, including password reuse. An attacker with employee's credentials can access sensitive data or functionality & give full control over their online account. Moreover, in cloud, organisations lack ability to identify & respond to these threats.

⑤ Lack of Visibility :- An organisation's ~~cloud based resources~~ are located outside of corporate network & run on infrastructure that company doesnot own. This can limit an organisation's ability to monitor their cloud-based resources & protect them against attack.

⑥ External Sharing of data :- While easy data sharing is an asset, it can also be a cloud security issue. The shared link can be forwarded to someone else, stolen as part of cyberattack or cybercriminal provides unauthorised access to ~~shared~~ shared resource.

8 Mark Questions

same Ans 6

Ques 13:- Discuss about each protocol utilised in cloud services & also the architecture of software defined networking with open stack. Discuss open stack security with its diagram properly.

Ans:-

Protocols is the set of rules that allows 2 electronic items to connect and exchange information to one another.

Cloud Computing Protocols are :-

① GOSSIP PROTOCOL :-
It is a communication protocol.
It is used for failure detection, monitoring and messaging.

② CONNECTION-LESS NETWORK PROTOCOL :-
It works on layer-3 protocol OSI Model.
It works on mechanism of fragmentation (data unit identification, length of data + offset address)

③ STATE ROUTING PROTOCOL :-
A router communicate with each other, routing algo is used to choose the path to route info.
for eg: IP and IPX

④ INTERNET GROUP MANAGEMENT PROTOCOL
It is a communication protocol used to multi-cast the data to nodes in network via router.
It can be used for streaming video, gaming over cloud.

⑤ SECURE SHELL PROTOCOL
It is cryptographic network protocol which allows remote login securely over internet.

⑥ COVERAGE ENHANCED ETHERNET PROTOCOL
It solves network traffic & packet loss issues.

⑦ EXTENSIBLE MESSAGING AND PRESENCE PROTOCOL
used for publish subscriber system, video & file transfer in cloud.

⑧ ADVANCED MESSAGE QUEUING PROTOCOL

Its a wireless protocol which provide description format of data send on network.

It provides a gurantees of message delivery & work on application layer.

⑨ ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

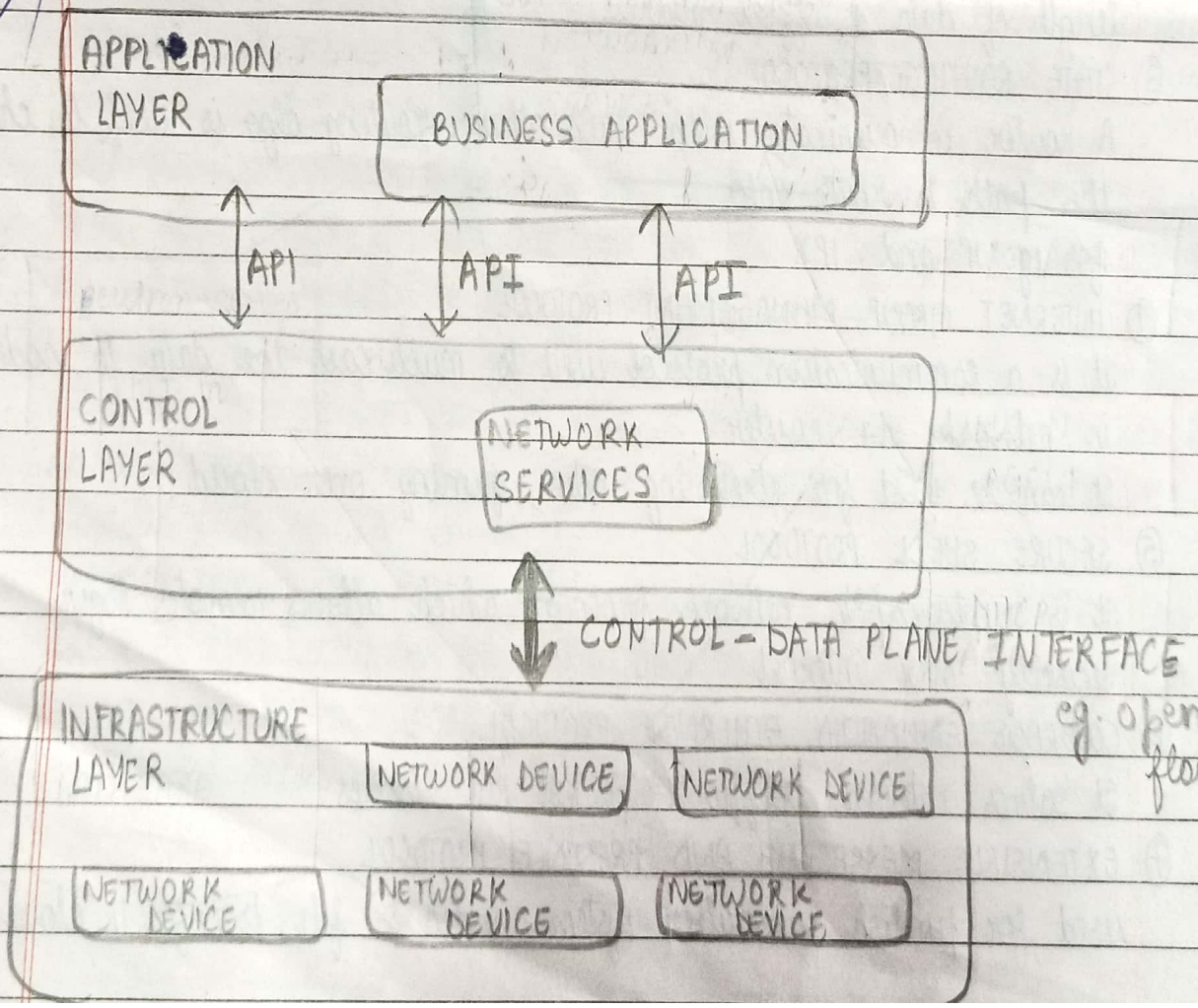
It supports load balancing on parallel linked site.

⑩ MEDIA TRANSFER PROTOCOL

It transfers the media files, audio files, metadata to & from portable devices over a cloud.

Also used for downloading photographs from cloud.

(b) ARCHITECTURE OF SDN WITH OPEN STACK

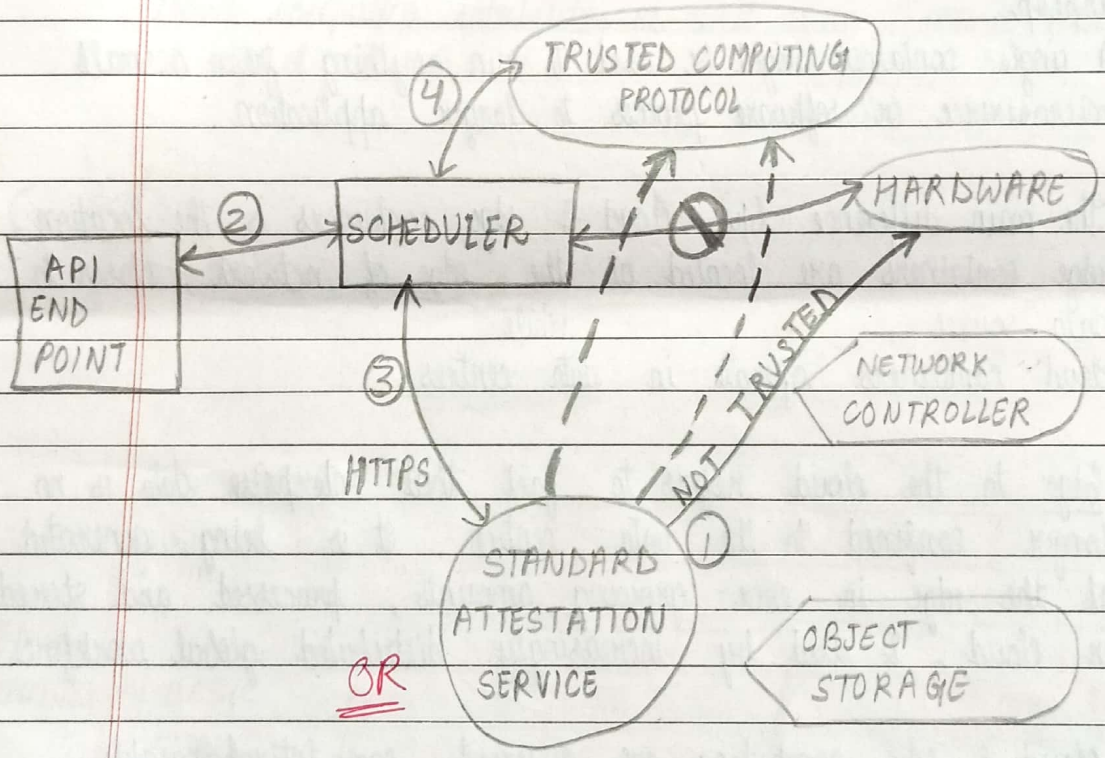


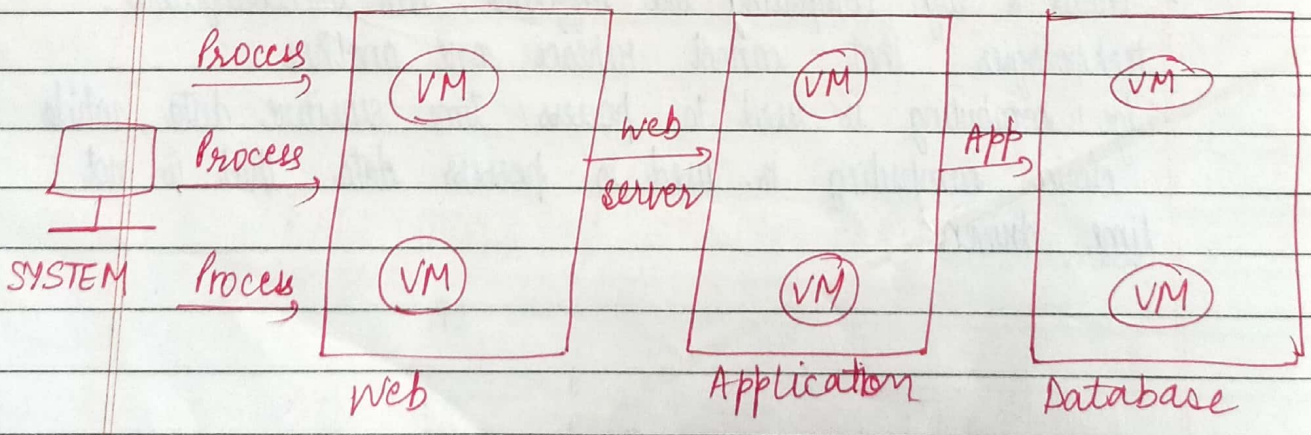
SDN Architecture depicts logical view of SDN.

→ The infrastructural layer sends control information via interface to SDN control software in control layer, where abstracted view of network is created & configuration or status of underlying infrastructure is maintained. Network services are created leveraging the information contained in SDN controller.

(c) OPEN STACK SECURITY

Open stack compute can be integrated with various third party technologies to increase security.





edge computing → cloud computing → IOT devices
↓ simplified bandwidth/latency reduce
saves time fast saves cost
real time data

CH 9]

Ques 14:- Discuss with diagram and examples about Containers and edge computing with openstack in cloud service.

Ans:-

Containers are packages of software that contain all of necessary elements to run in any environment.
Containers virtualise the OS & run anywhere from a private data centre to public cloud or even on developer's personal laptop.
A single container might be used to run anything from a small microservice or software process to larger application.

* The main difference btw cloud & edge containers is the location. Edge containers are located at the edge of network, closer to data source, while cloud containers operate in data centres.

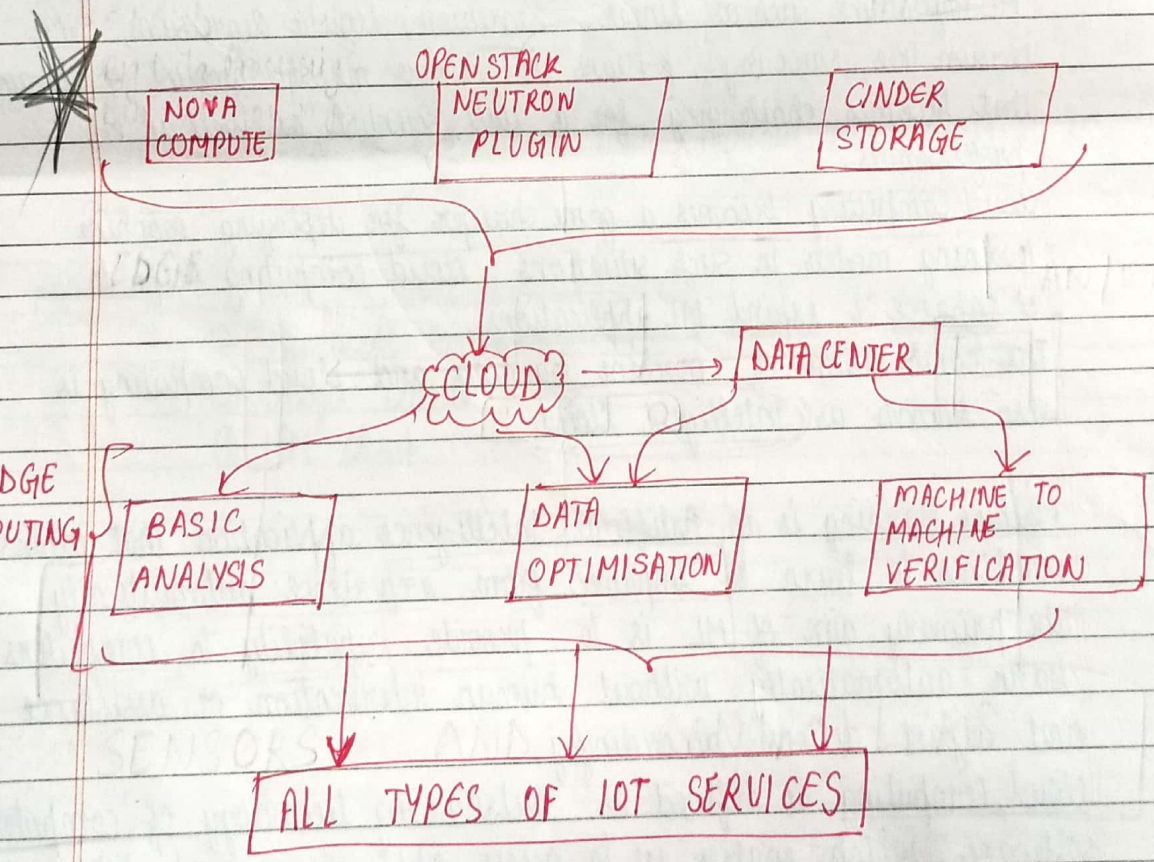
→ Edge to the cloud refers to fact that enterprise data is no longer confined to the data centre. It is being generated at the edge in ever-growing amounts, processed and stored in cloud, & used by increasingly distributed global workforce.

→ Cloud & edge computing are different, non-interchangeable technologies that cannot replace one another.
Edge computing is used to possess time sensitive data, while cloud computing is used to possess data that is not time driven.

→ storage

Edge computing is already in use all around us - from wearable on your wrist to computers parsing intersection traffic flow.
other examples include smart utility grid analysis, safety monitoring of oil rigs, streaming video optimization & drone enabled crop management.

* Edge computing offers application developers & service providers cloud computing capabilities as well as an IT service environment at edge of network.



edge computing → local devices instead of cloud.
on

Date
Page

Ques 15:- "Cloud being best way to deliver application for new technologies specifically cloud with Machine learning is used at vast scenario." Support this real world statement about cloud by suitable answer.

Ans:-

In this technology-driven time, Machine learning and Cloud computing are most powerful technologies worldwide. Both these technologies play a crucial role for small & big organisations to grow their businesses.

Machine learning helps users make predictions & develop algorithms that can automatically learn by using historical data. However, various ML Algorithms such as Linear Regression, Logistic Regression, SVM, Decision Tree, Naive Bayes, K-Means etc. require massive amount of storage that becomes challenging for a data scientist as well as ML professionals.
Cloud computing becomes a game changer for deploying machine learning models in such situations. Cloud computing helps to enhance & expand ML applications.
The combination of machine learning and cloud computing is also known as Intelligent Cloud.

Machine learning is an Artificial Intelligence application that allows machines to learn & improve from experience automatically. The primary aim of ML is to provide capability to computers learn automatically without human intervention or assistance and adjust actions accordingly.
Cloud computing is defined as outsourcing technology of computer software, which enables us to access applications and data remotely. One can enjoy its services online without installing any software.

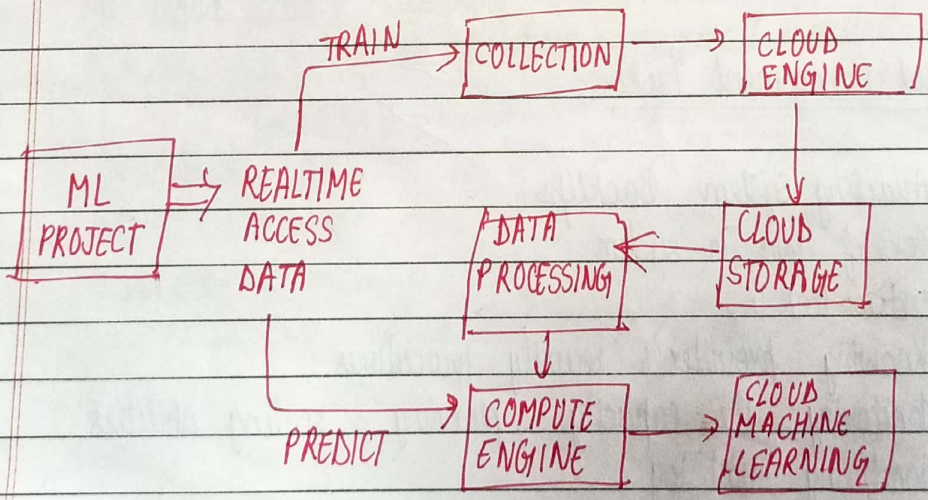
ML → data → CLOUD
+
INTELLIGENT CLOUD

Date
Page

* The main connection b/w machine learning & cloud computing is resource demand. ML requires lot of processing power, data storage and many servers simultaneously to work on an algorithm.
→ Then, cloud computing plays a significant role in providing new servers with pre-defined data & changing resources over cloud.
→ Cloud computing is used for computation purposes, ML needs a lot of computational powers to create sample data, & not everyone has access to many strong machines. ML finds task scheduling & storage in cloud computing.

Advantages:- ① Pay-per-use model.
② provides flexibility to work with Machine learning functionalities without having advanced data skills.
③ helps ease of experiment with various ML technologies & scales up as projects go into production & demand increases.

Platforms:- ① AWS - most popular; developed by Amazon.
② Microsoft Azure
③ Google Cloud
④ IBM Cloud



Ques 16→ "Control on everything is mandatory and to follow this in cloud we have a specific rule of management." In this problem which specific problem is to be discussed, identify & discuss in detail about role of management with proper examples and diagram. rule

Ans:- Cloud Management refers to how an organisation controls its applications & services in the cloud, from workload performance to security, costs & more.
It makes it possible to track & allocate the company's expenses in cloud computing, generate reports & predict future loads. Thus, it provides accurate cost management, forecasting & reporting.

(CMP) Cloud Management Platform:- is a software solution that has a robust and extensive set of APIs that allow it to pull data from every corner of IT infrastructure. A CMP allows an IT organization to establish a structured approach to security & IT governance that can be implemented across organisation's cloud environment.

Cloud Management Tasks:-

1. Auditing System Backups
2. Flow of data in system
3. Vendor Lock in
4. Knowing provider's security procedures
5. Monitoring, the capacity, planning & scaling abilities.
6. Monitoring audit log.
7. Solution Testing & Validation