MCQ questions

1- Amazon Web Services falls into which of the following cloud-computing category?

a) Platform-as-service

b) Software-as-Service

c) Infrastructure-as-service

d) Backen-as-Service

2- What are the different types of instances?

a) General purpose

b) Computer Optimized

c) Storage Optimized

d) All of the above

3- What are the advantages of auto-scaling?

a) Better availability)
b) Offers fault tolerance)
c) Better cost management
d) All of the above

4- What are the Authentication in AWS?

a) User Name/Password
b) Access Key,c
c) Access Key/ Session Token
d) All of the above

5- Which of the following is a billing and account management service?

a) Amazon Elastic MapReduce

b) Amazon Mechanical Turk

c) Amazon DevPay

d) Multi-Factor authentication

6- S3 stands for Simple Storage Service

a) True

b) False

7- Which of the following services you would not use to deploy an app?

a) Elastic Beanstalk

b) Lambda

c) Opsworks

d)CloudFormation

8- Amazon EC2 provides virtual computing environments, known as:

a) Chunks
b) Instances
c) Messages
d) None of the mentioned

9- Which of the following is a system for creating block level storage devices that can be used for Amazon Machine Instances in EC2?

a) CloudWatch
b) Amazon Elastic Block Store
c) AWS Import/Export
d) All of the mentioned

10- Which of the following is Cloud Platform by Amazon?

a) Azure
b) AWS
c) Cloudera
d) All of the mentioned

11- Which model consists of the particular types of services that you can access on a cloud computing platform?

a) Service
b) Deployment
c) Application
d) None of the mentioned

12- Which one is not an AWS pricing model

a) Reserved Instance
b) Available Instance
c) Spot Instance
d) On demand Instance

13- When will you incur costs with an Elastic IP address (EIP)?

a) When an EIP is allocated
b) When it is allocated and associated with a running instance
c) When it is allocated and associated with a stopped instance
d) Costs are incurred regardless of whether the EIP is associated with a running instance.

14- Are the Reserved Instances available for Multi-AZ Deployments?

a) Multi-AZ Deployments are only available for Cluster Compute instances types
b) Available for all instance types
c) Only available for M3 instance types
d) Not Available for Reserved Instances

15- Which of the following is an optional security control that can be applied at the subnet layer of a VPC?

a) Network ACL
b) Security Group
c) Firewall
d) Web application firewall

16- What happens when you create a new Amazon VPC?

a) A main route table is created by default
b) Three subnets are created by default—one for each Availability Zone
c) Three subnets are created by default in one Availability Zone
d) An IGW is created by default.

17- What aspect of an Amazon VPC is stateful?

a) Network ACLs
b) Security groups
c) Amazon DynamoDB
d) Amazon S3

18- Which of the following is the security protocol supported by Amazon VPC?

a) SSH
b) Advanced Encryption Standard (AES)
c) Point-to-Point Tunneling Protocol (PPTP)
d) IPsec

19- Which AWS database service is best suited for traditional Online Transaction Processing (OLTP)?

a) Amazon Redshift
b) Amazon Relational Database Service (Amazon RDS)
c) Amazon Glacier
d) Elastic Database

20- What is the minimum size subnet that you can have in an Amazon VPC?

a) /24
b) /26,
c) /28
d) /30

21- You create a new subnet and then add a route to your route table that routes traffic out from that subnet to the Internet using an IGW. What type of subnet have you created?

a) An internal subnet
b) A private subnet
c) An external subnet
d) A public subnet

Short questions

1- Explain what AWS is?

AWS stands for Amazon Web Service; it is a collection of remote computing services also known as a cloud computing platform. This new realm of cloud computing is also known as IaaS or Infrastructure as a Service.

2- Explain what S3 is?

S3 stands for Simple Storage Service. You can use S3 interface to store and retrieve any amount of data, at any time and from anywhere on the web. For S3, the payment model is "pay as you go."

3- What is AMI?

AMI stands for Amazon Machine Image. It's a template that provides the information (an operating system, an application server, and applications) required to launch an instance, which is a copy of the AMI running as a virtual server in the cloud. You can launch instances from as many different AMIs as you need.

4- Mention what the relationship between an instance and AMI is?

From a single AMI, you can launch multiple types of instances. An instance type defines the hardware of the host computer used for your instance. Each instance type provides different computer and memory capabilities. Once you launch an instance, it looks like a traditional host, and we can interact with it as we would with any computer.

5- What does an AMI include?

An AMI includes the following things

A template for the root volume for the instance

Launch permissions decide which AWS accounts can avail the AMI to launch instances

A block device mapping that determines the volumes to attach to the instance when it is launched

6- How can you send a request to Amazon S3?

Amazon S3 is a REST service, and you can send a request by using the REST API or the AWS SDK wrapper libraries that wrap the underlying Amazon S3 REST API.

7- What are key-pairs in AWS?

Key-pairs are secure login information for your virtual machines. To connect to the instances, you can use key-pairs which contain a public-key and private-key.

8- What are the different types of instances?

General purpose, Computer Optimized, Memory Optimized, Storage Optimized, Accelerated Computing

9- What are the roles?

Roles are used to providing permissions to entities which you can trust within your AWS account. Roles are very similar to users. However, with roles, you do not require to create any username and password to work with the resources.

10- What is VPC?

VPC stands for Virtual Private Cloud. It allows you to customize your networking configuration. It is a network which is logically isolated from another network in the cloud. It allows you to have your IP address range, internet gateways, subnet and security groups.

11- What is AWS Lambda?

Lambda is an Amazon compute service which allows you to run code in the AWS Cloud without managing servers

12- What is a Hypervisor?

A Hypervisor is a kind of software that enables Virtualization. It combines physical hardware resources into a platform which is delivered virtually to one or more users. XEN is the Hypervisor for EC2.

13- What is the use of Subnets?

When a network has more number of HOSTS, managing these hosts can be tedious under a single large network. Therefore, we divide this large network into easily manageable sub-networks (subnets) so that managing hosts under each subnet becomes easier.

14- What are all the different connectivity options available for your VPC in AWS?

Internet Gateway, Virtual Private Gateway, NAT, Endpoints, Peering Connections.

15- What is an auto-scaling and what are the components?

Auto scaling allows you to automatically scale-up and scale-down the number of instances depending on the CPU utilization or memory utilization. There are 2 components in Auto scaling, they are Auto-scaling groups and Launch Configuration.

16- What is CloudWatch?

CloudWatch is a monitoring tool that you can use to monitor your various AWS resources. Like health check, network, Application, etc

17- What is glacier?

Glacier is the back up or archival tool that you use to back up your data in S3.

18- What are NAT gateways?

NAT stands for Network Address Translation. NAT gateways enables instances in a private subnet to connect to the internet but prevent the internet from initiating a connection with those instances

19- What are the benefits of auto scaling?

Better fault tolerance, Better availability, Better cost management

20- What are security groups in AWS?

Security groups acts as a firewall that contains the traffic for one or more instances. You can associate one or more security groups to your instances when you launch then. You can add rules to each security group that allow traffic to and from its associated instances. You can modify the rules of a security group at any time, the new rules are automatically and immediately applied to all the instances that are associated with the security group

21- What is mean by Region in AWS

Region: An independent collection of AWS resources in a defined geography. A collection of Data centers (Availability zones). All availability zones in a region connected by high bandwidth.

22- What is mean by Availability zone in AWS

An Availability zone is a simply a data centre. Designed as independent failure zone. High speed connectivity, Low latency.

23- How to access AWS Platform?

AWS Console, AWS CLI (Command line interface), AWS SDK (Software Development Kit)

24- What are the benefits in EC2?

On-Demand Instances, Reserved Instances, Spot Instances, Dedicated Host

25- What are the pricing models in EC2 ?

On-demand, Spot instances, scheduled instances, reserved instances, Dedicated instances, Dedicated hosts, Saving plans., Capacity reservations

26- What are the types you have in storage gateway ?

File gateway, Volume gateway, Tape gateway

27- Difference between Security Groups and ACLs in a VPC?

A Security Group defines which traffic is allowed TO or FROM EC2 instance. Whereas ACL, controls at the SUBNET level, scrutinize the traffic TO or FROM a Subnet.

28- What are EBS volumes?

it stands for Elastic Block Stores. They are persistent volumes that you can attach to the instances. With EBS volumes, your data will be preserved even when you stop your instances, unlike your instance store volumes where the data is deleted when you stop the instances.

29- Name some of the DB engines which can be used in AWS RDS

MS-SQL DB, MariaDB, MYSQL DB, Oracle DB, Postgre DB

30- Explain how the buffer is used in Amazon web services?

The buffer is used to make the system more robust to manage traffic or load by synchronizing different component. Usually, components receive and process the requests in an unbalanced way. With the help of buffer, the components will be balanced and will work at the same speed to provide faster services.

4&6&8 marks questions

1- Mention what the key components of AWS are?

The key components of AWS are

Route 53: A DNS web service

Simple E-mail Service: It allows sending e-mail using RESTFUL API call or via regular SMTP

Identity and Access Management: It provides enhanced security and identity management for your AWS account

Simple Storage Device or (S3): It is a storage device and the most widely used AWS service

Elastic Compute Cloud (EC2): It provides on-demand computing resources for hosting applications. It is handy in case of unpredictable workloads

Elastic Block Store (EBS): It offers persistent storage volumes that attach to EC2 to allow you to persist data past the lifespan of a single Amazon EC2 instance

CloudWatch: To monitor AWS resources, it allows administrators to view and collect key Also, one can set a notification alarm in case of trouble.

2- While connecting to your instance what are the possible connection issues one might face?

The possible connection errors one might encounter while connecting instances are

Connection timed out

User key not recognized by the server

Host key not found; permission denied

An unprotected private key file

Server refused our key or no supported authentication method available

Error using Midterm on Safari Browser

Error using Mac OS X RDP Client

3- Explain can you vertically scale an Amazon instance? How?

Yes, you can vertically scale on Amazon instance. For that Spin up a new larger instance than the one you are currently running

Pause that instance and detach the root webs volume from the server and discard

Then stop your live instance and detach its root volume

Note the unique device ID and attach that root volume to your new server

And start it again

4- List out The Advantages of AWS.

- AWS allows organizations to use the already familiar programming models, operating systems, databases, and architectures.
- It is a cost-effective service that allows you to pay only for what you use, without any up-front or long-term commitments.
- You will not require to spend money on running and maintaining data counteroffers fast deployments
- You can easily add or remove capacity.
- You are allowed cloud access quickly with limitless capacity.
- Total Cost of Ownership is very low compared to any private/dedicated servers.
- Offers Centralized Billing and management Offers Hybrid Capabilities
- Allows you to deploy your application in multiple regions around the world with just a few clicks

5- List out The Disadvantages of AWS.

- If you need more immediate or intensive assistance, you'll have to opt for paid support packages.
- Amazon Web Services may have some common cloud computing issues when you move to a cloud. For example, downtime, limited control, and backup protection.
- AWS sets default limits on resources which differ from region to region. These resources consist of images, volumes, and snapshots.
- Hardware-level changes happen to your application which may not offer the best performance and usage of your applications.

6- How does AWS Lambda work? Explain with Steps.

Step 1: First upload your AWS Lambda code in any language supported by AWS Lambda. Java, Python, Go, and C# are some of the languages that are supported by AWS lambda.

Step 2: These are some AWS services which allow you to trigger AWS Lambda.

Step 3: AWS Lambda helps you to upload code and the event details on which it should be triggered.

Step 4: Executes AWS Lambda Code when it is triggered by AWS services:

Step 5: AWS charges only when the AWS lambda code executes, and not otherwise.

This will happen in the following scenarios:

Upload files in an S3 bucket

When HTTP get/post endpoint URL is hit

For adding/modifying and deleting Dynamo DB tables

In the process of data streams collection

Push notification

Hosting of website

Email sending

7- What is AWS Certificate Manager?

AWS Certificate Manager (ACM) manages the complexity of extending, provisioning, and regulating

certificates granted over ACM (ACM Certificates) to your AWS-based websites and forms. You work ACM to petition and maintain the certificate and later practice other AWS services to provision the ACM Certificate for your website or purpose. As designated in the subsequent instance, ACM Certificates are currently ready for a performance with only Elastic Load Balancing and Amazon CloudFront. You cannot handle ACM Certificates outside of AWS

8- List out and Explain Features of EC2

- Reliable − Amazon EC2 offers a highly reliable environment where replacement of instances is rapidly possible. Service Level Agreement commitment is 99.9% availability for each Amazon EC2 region.
- Designed for Amazon Web Services − Amazon EC2 works fine with Amazon services like Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon SQS. It provides a complete solution for computing, query processing, and storage across a wide range of applications.
- Secure − Amazon EC2 works in Amazon Virtual Private Cloud to provide a secure and robust network to resources.
- Flexible Tools − Amazon EC2 provides the tools for developers and system administrators to build failure applications and isolate themselves from common failure situations.

- Inexpensive − Amazon EC2 wants us to pay only for the resources that we use. It includes multiple purchase plans such as On-Demand Instances, Reserved Instances, Spot Instances, etc. which we can choose as per our requirement.

9- Explain in detail about AWS VPC and List out Services that can be used with VPC.

Amazon Virtual Private Cloud (VPC) allows the users to use AWS resources in a virtual network. The users can customize their virtual networking environment as they like, such as selecting own IP address range, creating subnets, and configuring route tables and network gateways.

The list of AWS services that can be used with Amazon VPC are :

- Amazon EC2
- Amazon Route 53
- Amazon WorkSpaces
- Auto Scaling
- Elastic Load Balancing
- AWS Data Pipeline
- Elastic Beanstalk
- Amazon Elastic Cache
- Amazon EMR
- Amazon OpsWorks
- Amazon RDS
- Amazon Redshift

10- Is one Elastic IP address enough for every instance that I have running?

Depends! Every instance comes with its own private and public address. The private address is associated exclusively with the instance and is returned to Amazon EC2 only when it is stopped or terminated. Similarly, the public address is associated exclusively with the instance until it is stopped or terminated. However, this can be replaced by the Elastic IP address, which stays with the instance as long as the user doesn't manually detach it. But what if you are hosting multiple websites on your EC2 server, in that case you may require more than one Elastic IP address.

11- Can I connect my corporate datacentre to the Amazon Cloud? Is it possible to change the private IP addresses of an EC2 while it is running/stopped in a VPC?

Yes, you can do this by establishing a VPN (Virtual Private Network) connection between your company's

network and your VPC (Virtual Private Cloud), this will allow you to interact with your EC2 instances as if they were within your existing network.

Primary private IP address is attached with the instance throughout its lifetime and cannot be changed, however secondary private addresses can be unassigned, assigned or moved between interfaces or instances at any point.

12- Can user run more than one DB instance for Amazon RDS for free?

Yes. User can run more than one Single-AZ Micro database instance, that too for free! However, any use

exceeding 750 instance hours, across all Amazon RDS Single-AZ Micro DB instances, across all eligible

database engines and regions, will be billed at standard Amazon RDS prices. For example: if you run two

Single-AZ Micro DB instances for 400 hours each in a single month, you will accumulate 800 instance hours of usage, of which 750 hours will be free. You will be billed for the remaining 50 hours at the standard Amazon RDS price.

13- What happens if user application stops responding to requests in beanstalk?

AWS Beanstalk applications have a system in place for avoiding failures in the underlying infrastructure. If an Amazon EC2 instance fails for any reason, Beanstalk will use Auto Scaling to automatically launch a new instance. Beanstalk can also detect if your application is not responding on the custom link, even though the infrastructure appears healthy, it will be logged as an environmental event (e.g., a bad version was deployed) so you can take an appropriate action.

14- Define and explain the three basic types of cloud services and the AWS products that are built based on them?

The three basic types of cloud services are:

Computing, Storage, Networking

- Computing - These include EC2, Elastic Beanstalk, Lambda, Auto-Scaling, and Lightsat.
- Storage - These include S3, Glacier, Elastic Block Storage, Elastic File System.
- Networking - These include VPC, Amazon CloudFront, Route53

15- What is a DDoS attack, and what services can minimize them?

DDoS is a cyber-attack in which the perpetrator accesses a website and creates multiple sessions so that the other legitimate users cannot access the service. The native tools that can help you deny the DDoS attacks on your AWS services are:

AWS Shield, AWS WAF, Amazon Route53, Amazon CloudFront, ELB, VPC

16- Name and explain some security products and features available in VPC? How do you monitor Amazon VPC?

- Security groups - This acts as a firewall for the EC2 instances, controlling inbound and outbound traffic at the instance level.
- Network access control lists - It acts as a firewall for the subnets, controlling inbound and outbound traffic at the subnet level.
- Flow logs - These capture the inbound and outbound traffic from the network interfaces in your VPC.

➢ You can monitor VPC by using:
  - CloudWatch and CloudWatch logs
  - VPC Flow Logs

17- What are the factors to consider while migrating to Amazon Web Services?

- Operational Costs - These include the cost of infrastructure, ability to match demand and supply, transparency, and others.
- Workforce Productivity
- Cost avoidance
- Operational resilience
- Business agility

18- What are the different types of load balancers in AWS? What are the different uses of the various load balancers in AWS Elastic Load Balancing?

- Application Load Balancer
- Used if you need flexible application management and TLS termination.
- Network Load Balancer
- Used if you require extreme performance and static IPs for your applications.
- Classic Load Balancer

➢ Used if your application is built within the EC2 Classic network

19- What are the different AWS IAM categories that you can control? What is the difference between an IAM role and an IAM user?

➢ Using AWS IAM, you can do the following:
  - Create and manage IAM users
  - Create and manage IAM groups
  - Manage the security credentials of the users
  - Create and manage policies to grant access to AWS services and resources

➢ The two key differences between the IAM role and IAM user are:

- An IAM role is an IAM entity that defines a set of permissions for making AWS service requests, while an IAM user has permanent long-term credentials and is used to interact with the AWS services directly.
- In the IAM role, trusted entities, like IAM users, applications, or an AWS service, assume roles whereas the IAM user has full access to all the AWS IAM functionalities.

20- What is Elastic Beanstalk? Mention a few benefits of the Elastic beanstalk

- Elastic Beanstalk is the best service offered by AWS for deploying and managing applications. It assists applications developed in Java, .Net, Node.js, PHP, Ruby, and Python. When you deploy the application, Elastic beanstalk built the selected supported platform versions and AWS services like S3, SNS, EC2, cloud watch and autoscaling to run your application.
- Following are the few benefits of the Elastic Beanstalk:
  - Easy and simple: Elastic Beanstalk enables you to manage and deploy the application easily and quickly.
  - Autoscaling: Beanstalk scales up or down automatically when your application traffic increases or decreases.
  - Developer productivity: Developers can easily deploy the application without any knowledge, but they need to maintain the application securely and user-friendly.
  - Cost-effective: No charge for Beanstalk. Charges are applied for the AWS service resources which you are using for your application.
  - Customization: Elastic Beanstalk allows users to select the configurations of AWS services that user want to use them for application development.
  - Management and updates: It updates the application automatically when it changes the platform. Platform updates and infrastructure management are taken care of by AWS professionals.

21- Explain the relationship between an instance and AMI? What des AMI include?

- A single Amazon Machine Image is used to launch multiple instances. The hardware of the host computer used by our instance is defined by the instance type. Each instance is provided with different capabilities of computing and memory. When the instance is launched, it looks like a traditional host and can be interacted like that of a computer.
- The Amazon Machine Image includes the following:
  - Launch permission decisions with which AWS accounts to launch the instances using AMI.
  - A block device mapping, when an instance is launched it determines the volumes to attach to that instance.
  - A template for the instance

22- What are the differences between NAT Gateways and NAT Instances?

Feature	NAT Gateway	NAT Instance
Availability	High	High
Bandwidth	Up to 45 Gbps	Depends on instance bandwidth
Maintenance	Managed by AWS	Managed by you
Performance	Very Good	Average
Cost	Number of gateways, duration and amount of usage	Number of instances, duration, amount and type of usage
Size and load	Uniform	As per your need
Security Groups	Cannot be assigned	Can be assigned

23- What is the best practice for encrypting cloud data?

User should encrypt data at rest and in motion. Encrypting “in motion” is already well known to user – the standards of HTTPS/SSL and IPSEC apply equally well in the data center and in the cloud.
Encrypting “at rest” means that the data must be encrypted when it resides on a disk, in a database, on a file system, in storage, and of course if it is backed up. In the real world, people have not always done this in data

centres – often relying on physical security as a replacement. In the cloud, physical security is no alternative – you must encrypt sensitive data.

This actually means data must be encrypted constantly as it is being written, and decrypted only when it is going to be used (i.e., just before a specific calculation, and only in memory). Standards such as Advanced Encryption Standard (AES) are commonly used for data encryption at rest

24- Does cloud encryption singlehandedly protect data?

If data is properly encrypted it is, in a sense, locked and cannot be used if it falls into the wrong hands. Unless, of course, those hands have a key.

Proper management of encryption keys is as important as the encryption itself. In fact, if you keep your encryption keys to yourself – you keep ownership of your data. This is an interesting and fundamental point – in the cloud you are outsourcing your infrastructure, but you can maintain ownership by keeping the encryption keys.

If encryption keys are stored alongside the data, any breach that discloses the data will also disclose the key to access it. If encryption keys are stored with cloud providers, they own your data.

25- Think of your data like a safe deposit box – would you leave your key with the banker? What if he gets robbed? What if his employees are paid to make copies of your key?

A best practice is split key encryption. With this method, your data is encrypted (e.g., with AES), and then the encryption key is split into parts. One part is managed with a cloud security provider and one part stays only with you. This way, only you control access to your data.

Even if your encrypted data is compromised, the perpetrators will not be able to decrypt it and it will be useless to them.

26- How does the cloud provider notify you of security breaches? How does the provider separate each client's data?

Even if the provider has proper security systems in place, a breach can happen at any moment. If a breach does occur, the provider needs to patch it out as soon as it can. Because security breaches can be either small or huge, not every breach will necessarily affect you, even if it's on a server you use. However, your provider should notify you of any security breach that happens on their data centers, especially if they potentially affect your data. Some cloud providers will inform users of breaches even if they affect an entirely different part of the data centre. If they do, it's helpful if the provider makes this known in its notifications. Just as important is breaches that can affect your data; providers need to tell you if your data is at risk. The best providers will outline steps you should (or need to) take to secure your data until the vendor contains the breach.

Most public cloud providers operate a multitenancy system, which means multiple users will store and operate data on the same server. This approach saves costs for the provider and utilizes their data centres to the fullest extent. In order to provide a multitenant system, the cloud provider must partition parts of their server to each individual user. The provider needs to have protocols in place to prevent users from accessing data on the same server that isn't part of their partition. They also need to take steps to stop data leakage from occurring and perform constant tests to ensure every partition is separated from each other.

27- Will User Data Kept Confidential When User Put Them on Cloud?

By default, when user store, use, share or communicate your data in the cloud, usually, user data is in a raw, unencrypted format, known as 'plaintext', unless you have encrypted user data before being saved or transmitted.

If user leave your data unencrypted, user will face the risk that anyone who gains access to your account can read, copy or delete your data. This leaves user data leaked or exposed to unauthorized individuals and entities. Thus, end-to-end data encryption including user emails if stored in Cloud servers, at rest, in-use and in motion, is a must.

On the other hand, from the provider's point-of-view, they will provide secure storage space and impose confidentiality obligations by limiting user access to those who are authorized to view, edit, add, and delete the data based on your requests. What's more, they will also protect the data from accidental or purposeful unauthorized access by internal or external actors.

Over and above that, user should gather the following information on data confidentiality policies, controls, practices, and technologies the provider has put in place like Access, Log Management, Data Management, Storage, Encryption, Storage.

28- If User Store Data on Cloud What about the Integrity?

As user might already be aware, data integrity, one of the key aspects in Information Security, means that the degree to which data is consistent, accurate and complete over its entire lifecycle.

To maintain it, user and the cloud provider must, hand-in-hand, provide such assurance.

- First, assure the data cannot be modified by an unauthorized individual, entity, or program. This could happen by deploying Access Controls through Access Control Matrix (ACM) or Access Control List (ACL) revealing username, role, privilege, menu, function and object. The forensic tool may be also needed to recover from the accidental deletion by authorized users. In addition, implement also another control, checksum, to verify integrity.
- Second, have data backup for occurrences like a power outage, database crash, storage failure. Given that the data is corrupted, try to identify the root cause then recover it in immediate. If it doesn't go through, restore correct data from the backup. Regardless of the storage media utilized for the backup, always put it in separate logical or even better physical premise and location. A secure, confidential, safe one, obviously. Security policy, both logical and physical, applied to primary and backup data must be the same.
- Third, implement algorithms and protocols namely Message-Digest algorithm 5 (MD5), Advanced Encryption Scheme (AES), Secure Hash Algorithm (SHA) and Rivest–Shamir–Adleman (RSA) to provide maximum levels of integrity management from any tampering or unauthorized access, specifically for data stored in the public cloud.
- Fourth, getting data integrity verified through IT Audit activities. It could be possibly conducted by internal (from your side/provider end) or external entities (third-party/independent). As the 3rd layer of defence inside an organization, IT Auditor will be assessing, validating and testing IT General Controls and IT Application Controls as necessary to verify the consistency, accuracy and completeness of certain static as well as dynamic data.