FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering.

Course, Subject & Experiment Details

Practical No:	8
Title:	To understand the Security practices available in public cloud platforms and to demonstrate various Threat detection, Data protection and Infrastructure protection services in AWS and Azure.
Name of the Student:	Warren Fernandes
Roll No:	8940
Date of Performance:	11/04/2022
Date of Submission:	11/04/2022

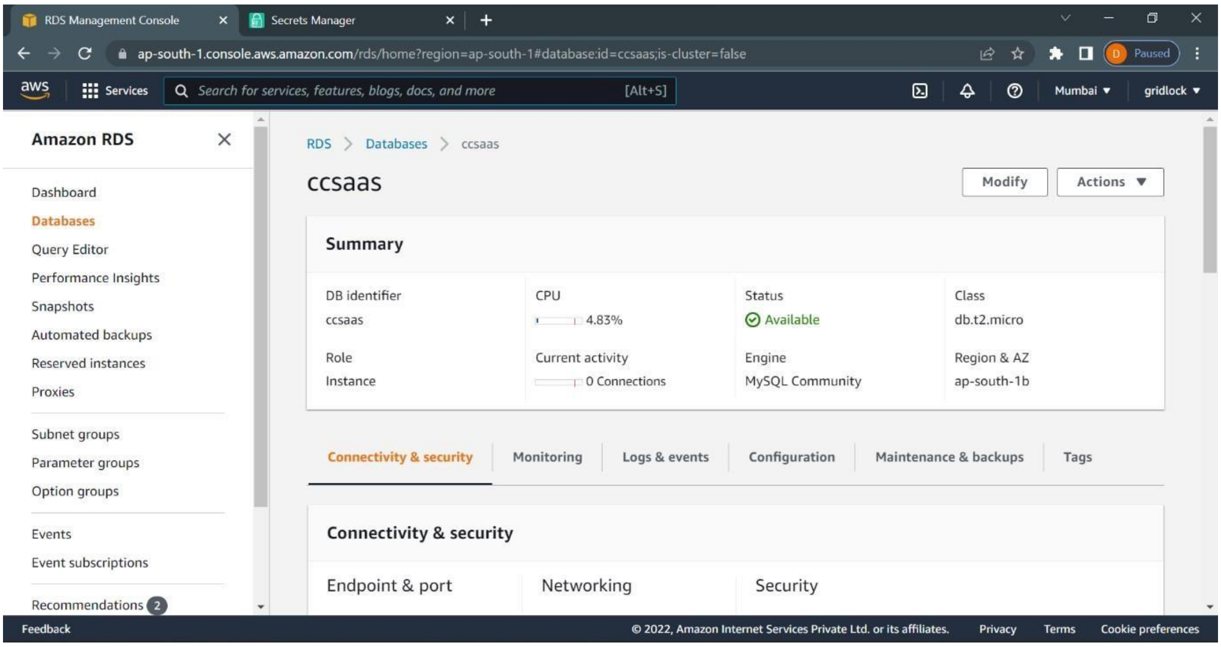
Evaluation:

Sr. No.	Rubric	Grade
1	On time submission/completion (2)	
2	Preparedness (2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher

1] Create an RDS database instance

- Allow public access and set backup period to zero days
- Enter the endpoint given in MySQL as hostname to setup a connection with RDS



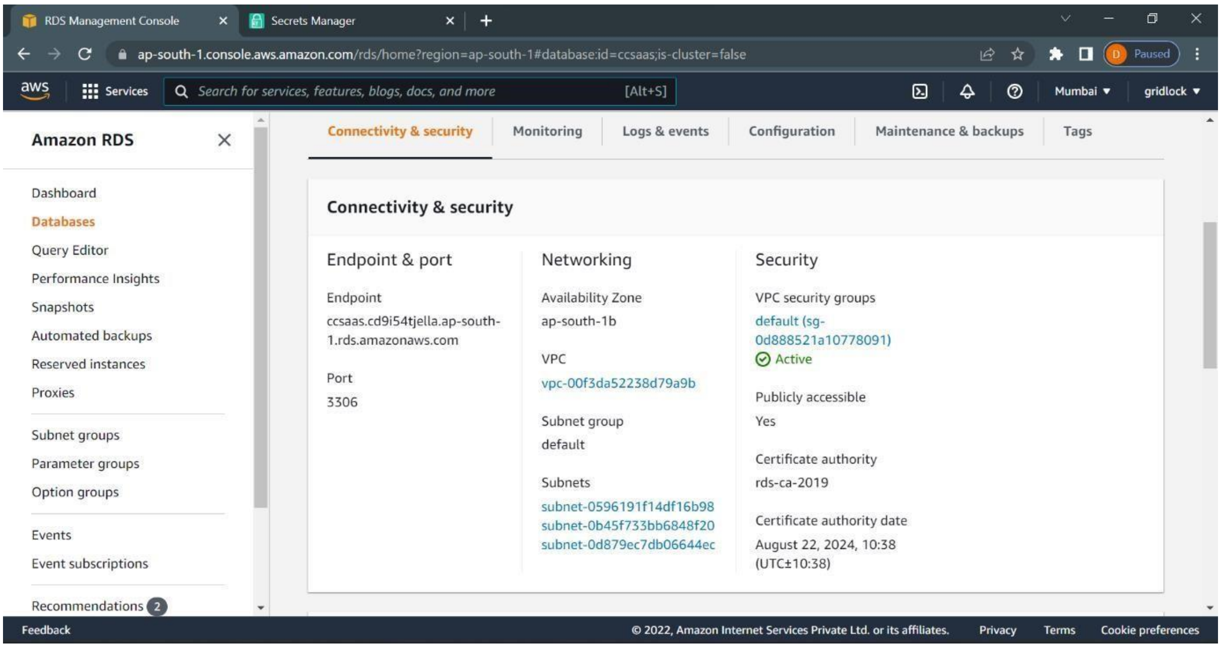
ccsaas

Summary

DB identifier	CPU	Status	Class
ccsaas	4.83%	Available	db.t2.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	ap-south-1b

Connectivity & security

Endpoint & port | Networking | Security



Connectivity & security

Endpoint & port

Endpoint
ccsaas.cd9i54tjella.ap-south-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
ap-south-1b

VPC
vpc-00f3da52238d79a9b

Subnet group
default

Subnets
subnet-0596191f14df16b98
subnet-0b45f733bb6848f20
subnet-0d879ec7db06644ec

Security

VPC security groups
default (sg-0d888521a10778091)
Active

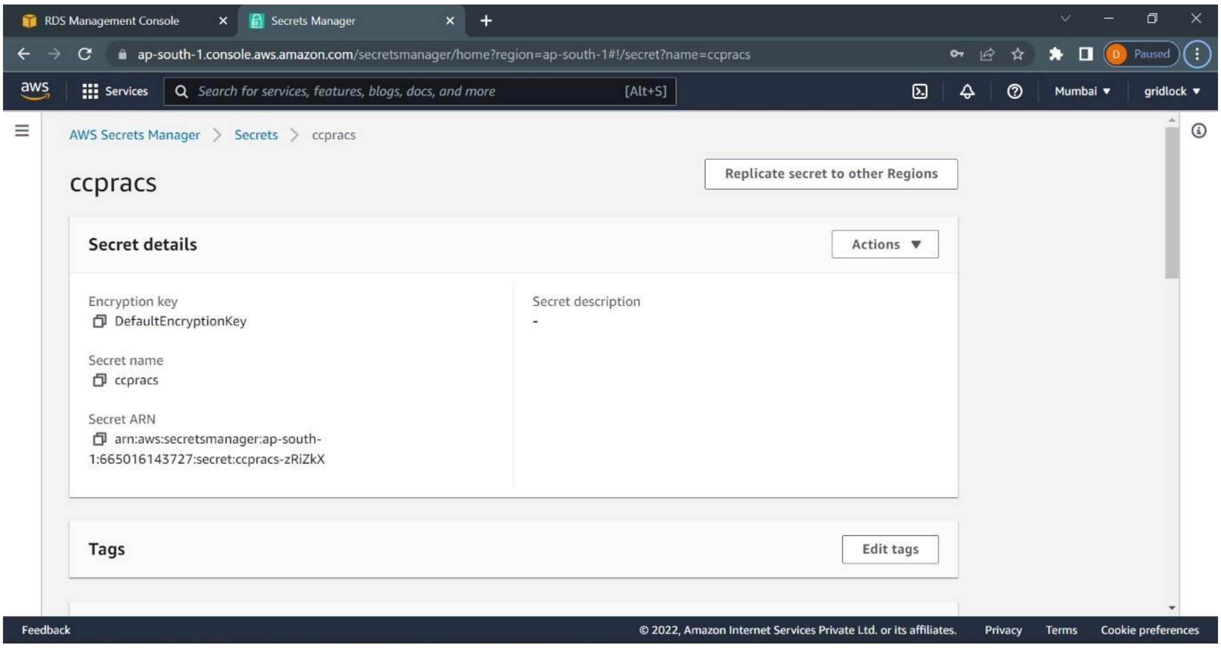
Publicly accessible
Yes

Certificate authority
rds-ca-2019

Certificate authority date
August 22, 2024, 10:38 (UTC±10:38)

2] Create a secret in AWS Secret Manager

- Select the corresponding RDS instance while creating a secret and set key rotation to a particular time period. 1 day in this case
- Enter the RDS instance’s username and password



AWS Secrets Manager > Secrets > ccpracs

ccpracs

Secret details

Encryption key
DefaultEncryptionKey

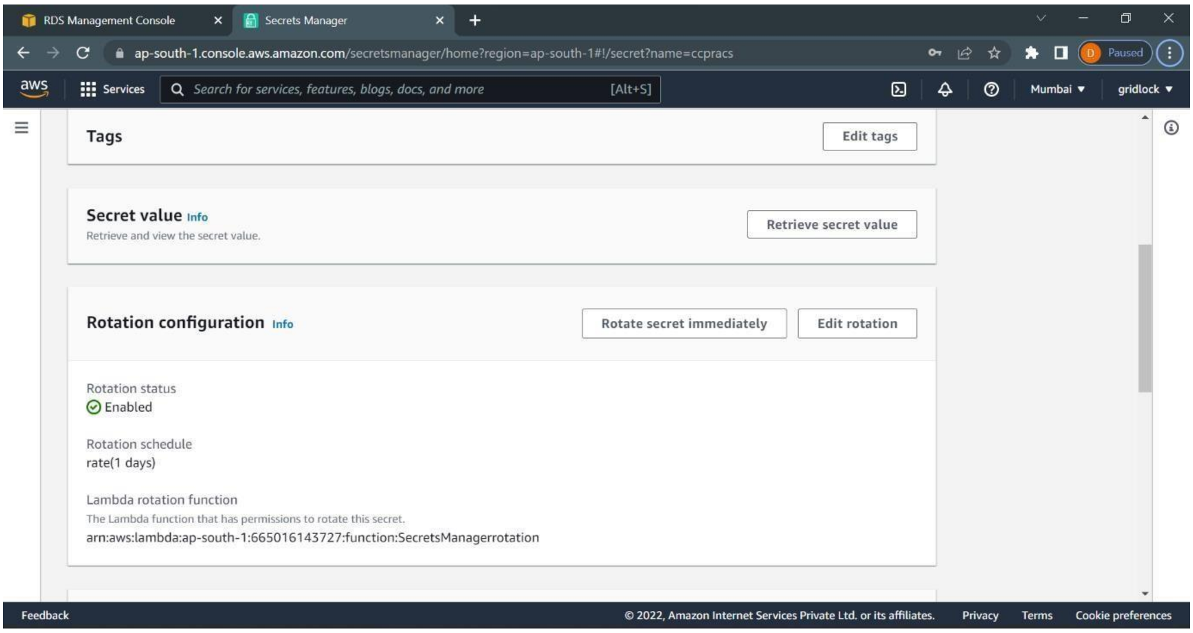
Secret name
ccpracs

Secret ARN
arn:aws:secretsmanager:ap-south-1:665016143727:secret:ccpracs-zRiZkX

Secret description
-

Tags

RDS Management Console
Secrets Manager
ap-south-1.console.aws.amazon.com/secretsmanager/home?region=ap-south-1#!/secret?name=ccpracs
Paused
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
gridlock
Replicate secret to other Regions
Actions
Edit tags
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences



Tags

Secret value Info
Retrieve and view the secret value.

Rotation configuration Info

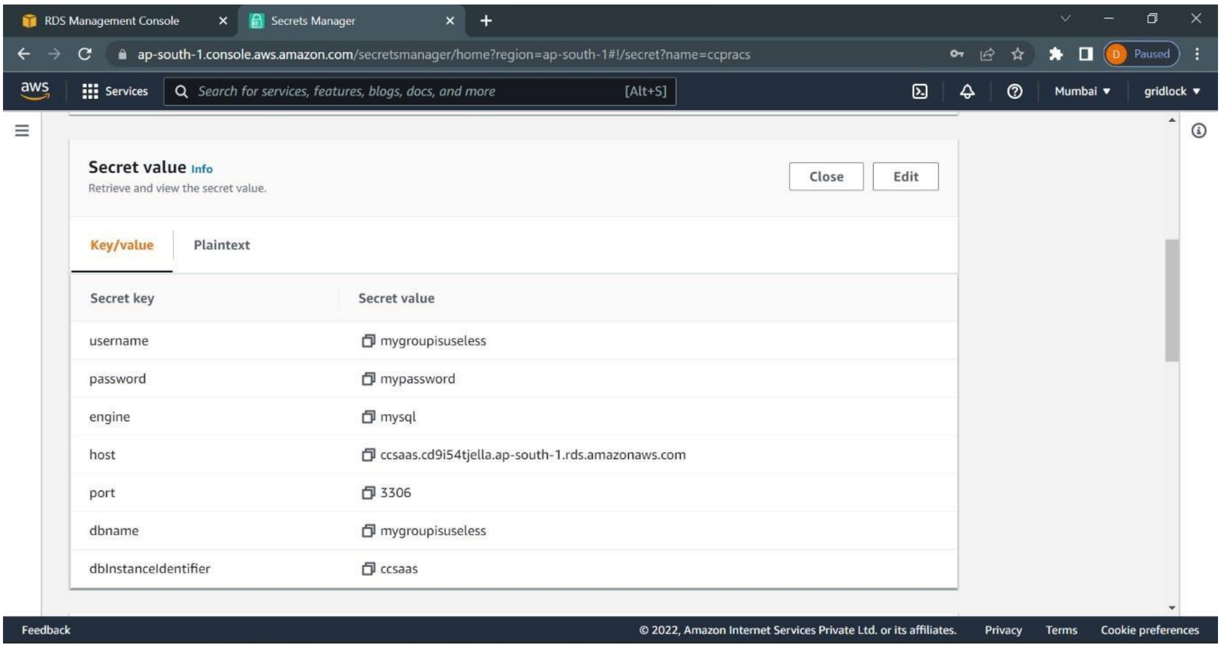
Rotation status
Enabled

Rotation schedule
rate(1 days)

Lambda rotation function
The Lambda function that has permissions to rotate this secret.
arn:aws:lambda:ap-south-1:665016143727:function:SecretsManagerrotation

RDS Management Console
Secrets Manager
ap-south-1.console.aws.amazon.com/secretsmanager/home?region=ap-south-1#!/secret?name=ccpracs
Paused
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
gridlock
Edit tags
Retrieve secret value
Rotate secret immediately
Edit rotation
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

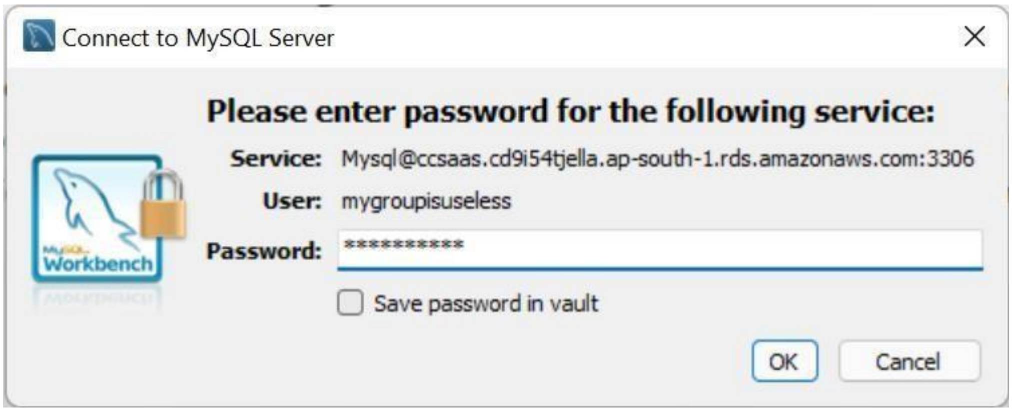
3] Retrieve secret value and enter in MySQL to gain access


RDS Management Console
Secrets Manager
ap-south-1.console.aws.amazon.com/secretsmanager/home?region=ap-south-1#!/secret?name=ccpracs
Paused
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai ▾
gridlock ▾
Close
Edit
Key/value
Plaintext
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Secret value Info

Retrieve and view the secret value.

Secret key	Secret value
username	mygroupisuseless
password	mypassword
engine	mysql
host	ccsaas.cd9i54tjella.ap-south-1.rds.amazonaws.com
port	3306
dbname	mygroupisuseless
dbInstanceIdentifier	ccsaas



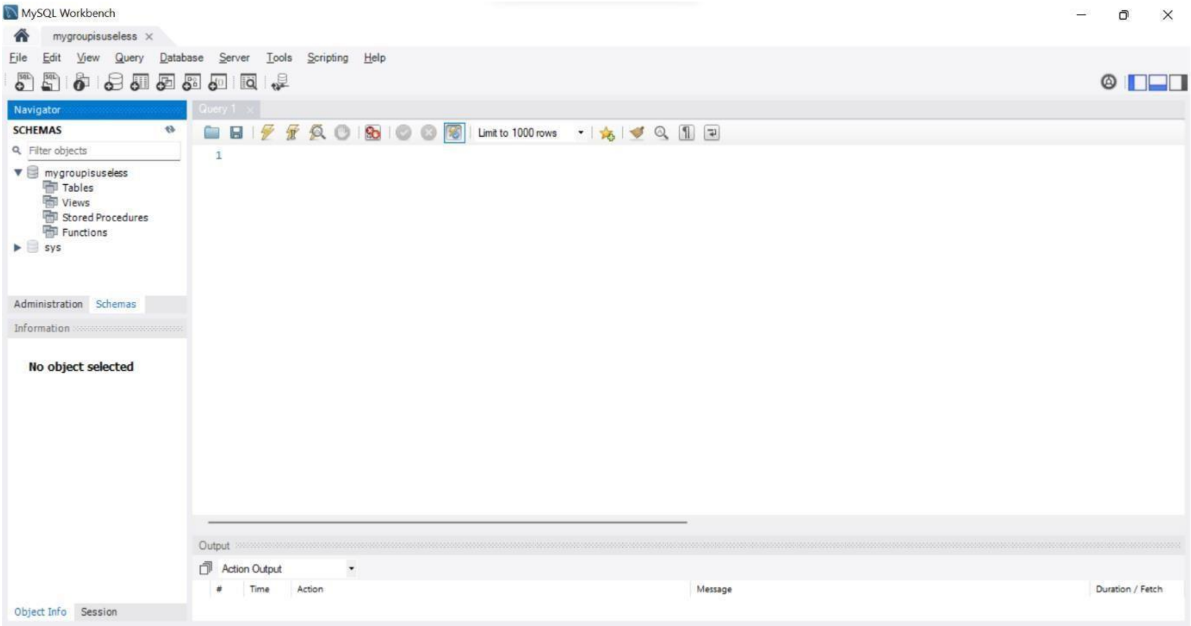
Please enter password for the following service:

Service: Mysql@ccsaas.cd9i54tjella.ap-south-1.rds.amazonaws.com:3306

User: mygroupisuseless

Password: **********

□ Save password in vault



4] We have successfully implemented Security as a Service in AWS Secrets Manager

Postlabs:

1. What is security threat when using a cloud based service?

- The high volume of data flowing between organizations and cloud service providers generates opportunities for accidental and malicious leaks of sensitive data to untrusted third parties.
- Human error, insider threats, malware, weak credentials and criminal activity contribute to most cloud service data breaches.
- The security threats when using a cloud based service are as follows:
  - **Cloud Misconfiguration:**
    Incorrect configurations of cloud infrastructure remains the top cause of cloud computing security breaches worldwide, seen from reported data breaches of the likes of Verizon and Adobe Creative Cloud.

  - **Denial of Service:**
    Attackers can flood an organization's cloud network with a large amount of web traffic, thus rendering resources unavailable to both customers and employees/staff. The bigger the chunk of infrastructure residing in the cloud, the more lethal a DoS attack will be.

  - **Insider threats:**
    Proper training and awareness is the key to mitigating insider attacks. Adhere to the principle of least privilege when architecting your environment's access controls to limit the damage employees can create and create a proper personnel offboarding protocol.

  - **Reduced Infrastructure visibility:**
    The nature of using a third party provider for computing means you hand over partial control to the cloud service provider (CSP). In this case, your organization does not own the physical infrastructure, making it more challenging to get full visibility of your infrastructure and resources uses, especially without the right technical expertise.

  - **Unauthorized Use of cloud:**
    Most major CSPs operate on a self-service model. This makes it easier for users to provision and de-provision workloads on the fly depending on their needs.

- **Insecure APIs:**
  You can have watertight controls within your infrastructure, but insecure application APIs can punch holes in your environment’s defenses and create an entryway. Many APIs have their own security vulnerabilities that, when exploited, can put your cloud environment at risk.

- **Compliance and regulation issues:**
  Organizations need to keep track of and comply with multiple regulations depending on their geographical operations and industry type. With new regulations appearing and older ones being updated as the landscape changes, it can be a challenge for organizations to keep up.

2. What are the security challenges in cloud computing?

The security challenges in cloud computing are as follows:

1. **Distributed Denial of Service Attacks:**
   A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

2. **Data breaches:**
   Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in all scenarios including private cloud, public cloud, and hybrid cloud situations), some of those security controls are relinquished to a trusted partner meaning cloud infrastructure can increase security risks. Choosing the right vendor, with a strong record of implementing strong security measures, is vital to overcoming this challenge.

3. **Data Loss:**
   When business critical information is moved into the cloud, it’s understandable to be concerned with its security. Losing cloud data, either through accidental deletion and human error, malicious tampering including the installation of malware (i.e. DDoS), or an act of nature that brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.

4. **Insecure access control points:**
   One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and particularly the application programming interfaces (APIs) users interact with aren't secure? Hackers can find and gain access to these types of vulnerabilities and exploit authentication via APIs if given enough time.

5. **Notifications and alerts:**
   Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud computing security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough data security and access management plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

3. How do you ensure security in cloud computing?

Security can be ensured in cloud computing through following ways:

1. **Use Encryption:**
   Encryption is a way to translate your business data into a secret code. Encrypted data is also referred to as cipher text and it is an effective way to ensure sensitive information remains uncompromised in the event of a data breach.

2. **Ask employees to use reliable passwords:**
   Weak Passwords can be like a free pass to your kingdom in the clouds. Creating reliable and strong passwords can protect your cloud data from a range of password-hacking tactics like brute force attack, dictionary attack, and fishing. These are common tactics used by cybercriminals day in and day out. Here are some tips that you can follow to create a strong password.

3. **Understand how Cloud Service Storage Works:**
   Enterprises have multiple options to choose from when it comes to storing business data on the cloud. It is very important to know exactly how different cloud services work and the best way to this is by reading the service agreement. This will offer a fair idea about the policies, technologies, applications, and controls offered to protect virtualized data.

4. **Use anti-virus software:**

The systems used to log into the cloud can be an opening for hackers too. In order to prevent business data from being exposed, make sure that the systems have antivirus software installed.

5. **Use local back-up:**
   Enterprises must consider creating a backup of critical data in secondary cloud storage or external storage device. This will ensure that an enterprise will always have a contingency plan against data thefts and related incidents.

4. What is the most effective security in cloud computing?

Intrusion prevention and detection systems (IDPS) are among some of the most effective cloud security tools on the market. They monitor, analyze, and respond to the network traffic across both on-premises and public cloud environments.

5. How can security problems be overcome in cloud computing?

Following ways can be adopted to overcome security problems in cloud computing:

1: Limit Your Cloud Computing Vendors

One of the major challenges in dealing with cloud-based solutions is that they can all have different security tools and processes—which makes them more difficult to manage. Here, finding ways to limit your selection of CSP vendors can be a major help.

2: Verify Your Access to Information about the Cloud Environment

Because visibility is so important to cybersecurity, it’s important to verify what information about the cloud environment you will have access to—preferably *before* signing an agreement. With greater visibility into the cloud environment, you can more easily track and control security.

3: Verify Security SLAs

Another thing to check before signing an agreement with a cloud service provider is what their service level agreements are regarding security. How quickly will they resolve a security breach after detection? How long will it take to restore normal service? Who is responsible for notifying affected parties?

Verifying these SLAs prior to signing an agreement can help ensure that they:

1. Meet your industry’s cybersecurity standards;
2. Will protect your business from untenably long service disruptions; and
3. Establish who is responsible for what following a data breach.

4: Check for Specific Security Measures

How will the CSP ensure that attackers don’t infiltrate your cloud environment? How will they limit the spread of attacks from one node on their network to another? Checking what security measures a cloud service provider has to offer is crucial for establishing:

- How prepared they are to protect your information;
- Their ability to meet compliance standards; and
- How easy or difficult it will be to incorporate the solution into your existing cybersecurity architecture.

5: Consult with a Cybersecurity Expert

If you are ever unsure of whether a cloud solution has the right security measures to protect your organization’s data, employees, and clients, consult with a cybersecurity expert.