P7. Analyse the most common problems Cloud Computing platform and solutions to these problems.

1. Common Cloud Issues

The instantaneous delivery of resources such as data and storage on demand is known as cloud computing. With a rapidly increasing market worth, it has demonstrated its innovative nature in the IT business.

1.1. Data Security and Privacy

One of the main concerns when moving to cloud computing is data security. Identity theft, data breaches, malware infections, and many other security problems in the cloud gradually erode consumers' faith in your apps.

 Solution

We ought to equip ourselves with a technique for safeguarding private data. By the way, we have to study up on account protection strategies and cyber security news. As an alternative, we could seek advice on account protection from friends and family members who are knowledgeable about information technology.

1.2. Cost Management

The hidden costs increase when resources are not optimized, such as when servers are not being used to their maximum capacity. Without even using the resources, the cost will go up if you switch on cloud services or an instance and neglect to turn it off over the weekend or when it's not in use.

 Solution

In order to minimize the amount of data that is used by the network that is outside of our control, we need proactively set a data traffic restriction.

1.3. Multi-Cloud Environments

Nearly 84% of these businesses rely on several clouds, and the majority of them employ hybrid cloud strategies. The infrastructure team frequently finds that this is challenging to handle and impedes their progress. Because of the variations across various cloud providers, the procedure frequently ends up being quite difficult for the IT staff.

 Solution

Multi-Cloud Environments ought to be restricted to larger businesses rather than startups. IT staff and time management will decline as a result.

1.4. Performance Challenges

Inadequate cloud performance has the potential to drive away customers and reduce revenue. A minor delay in the loading of an application or website might cause a significant decrease in the proportion of users. This delay may result from ineffective load balancing, which occurs when the server is unable to divide incoming traffic in a way that optimizes user experience.

 Solution

Users should be split into two groups: those who pay and those who don't. In terms of network connection speed, they will get precedence if they are a paying customer. Those who utilize it for free, on the other hand, will have network connection limitations. In other situations, we ought to boost network storage during high usage and reduce network traffic during off-peak hours. As a result, we will lessen the hardware burden on the network devices.

1.5. Interoperability and Flexibility

Because of the complexity required, moving between clouds does not offer the same flexibility. The management of data migration, initial security setup, and network configuration further compound the problems that arise when switching cloud solutions, ultimately decreasing flexibility.

 Solution

We need to set up separate private clouds for data transport and storage. We will therefore be able to send data over the cloud and lessen the issue of secure data. Prices will increase, but the issue will be resolved.

1.6. High Dependence on Network

Cloud computing handles massive volumes of data flow to and from the servers as it deals with the real-time supply of resources. Even if these resources and data are transferred across the network, this can be extremely vulnerable in situations when there is a sudden interruption or when bandwidth is restricted.Therefore, maintaining network bandwidth at a high cost is a significant difficulty for smaller businesses.

 Solution

The number of users connecting to the network should be determined, and then the network speed should be divided by the user's day, month, or time of day. Alternatively, we ought to go with a system that makes advantage of both data transmission and storage clouds. As a result, already produced, saved, and transferred data will move more quickly than freshly created data.

1.7. Lack of Knowledge and Expertise

It necessitates extensive subject-matter knowledge and proficiency. Even if there are many experts in the industry, they still need to stay up to date. Because of the wide discrepancy between supply and demand, cloud computing is a highly compensated profession. While there are many open positions, there aren't many skilled cloud engineers. Upskilling is therefore required in order for these individuals to actively comprehend, maintain, and create cloud-based applications with the fewest possible problems and the highest possible level of dependability.

 Solution

Light chores for humans can be performed by an artificial intelligence that we can construct. Alternatively, we educate a group of youth who possess sufficient understanding about fundamental security. From there, we gave a group of youths the task of protecting the outer layer. Rather, we carry out both.

2. Common issues of public, private, hybrid, community

Public Cloud Private Cloud Community

Cloud Hybrid Cloud

Easy to set up and use Easy Knowledge of

information technology Knowledge of

information technology Knowledge of information technology

Data security and

privacy Low High Relative high High

Data is controlled Medium High Relative high Relative high

Reliability Low High Relative high High

Extensible and flexible High High Stability High

Cost Cheap Expensive model, expensive cost Costs are shared with the community cheaper than the private model.

but more expensive than

the public model.

Depending on the

hardware No Depends on the

enterprise Depends on the

enterprise Depends on the

enterprise

3. Security Threats and Vulnerabilities

As previously stated, we will restrict the scope of our security assessment to the public cloud, which is the most widely used type of cloud. We first outline the fundamental security factors for this deployment paradigm before looking at and classifying the risks unique to CSPs and CSCs.

3.1. Basic Security Risk Considerations

When it comes to cloud computing, there are several places that might be hacked and therefore need to be guarded. Every space serves as a possible point of failure or assault. Five important such regions have been identified through risk analysis.

 Organizational Security Risks

Organizational risks are defined as those that have the potential to affect an organization's structure or the business as a whole. A CSP's CSPs may suffer if it goes out of business or is bought by another company. This is because any Service Level Agreements (SLAs) it may have had may have altered, and customers would then need to switch to a another CSP that better suits their needs.

 Physical Security Risks

An Overview of Security Concerns, Difficulties, and Solutions in Cloud Computing To stop illegal on-site access to CSC data, the cloud data center's physical location has to be guarded by the CSP. Firewalls and encryption are insufficient to prevent physical data theft. Since the CSP is in charge of the physical infrastructure, they should put in place and maintain the necessary infrastructure controls, such as network firewalls, staff training, and physical location security.

 Technological Security Risks

These hazards include malfunctions related to the CSP's hardware, technology, and services. Among the hazards associated with switching CSPs, or portability, are resource sharing and isolation issues in the public cloud with its multi-tenancy characteristics. It is advised that CSP do routine infrastructure audits and maintenance.

 Compliance and Audit Risks

These are legal risk factors. That is, the risks associated with incomplete information about jurisdiction, jurisdictional changes, contract provisions that are unlawful, and continuing legal challenges. For instance, depending on their location, certain CSPs can be required by law to provide sensitive data upon request from the government.

 Data Security Risks

There are several concerns related to data security that we must consider. The three primary attributes that require assurance are availability, confidentiality, and data integrity. We will go deeper into this topic in the next paragraph since the majority of cloud security efforts are directed at this area because it is the most vulnerable to compromise.

P8 Assess The Most Common Security Issues in Cloud Environments

1. Security Issues

Any unavoidable risk or weakness in your system that hackers may exploit to compromise systems or corrupt data is referred to be a security concern. This includes weaknesses in the people, procedures, and software that run your company and link it to clients, as well as servers and software.

1.1. Ransomware Attack

A ransomware assault aims to take complete control of important data. Your data is encrypted by the hacker, who then keeps it hostage until you pay a ransom for the decryption key that unlocks the contents. If you don't pay by the deadline, the attacker could even obtain sensitive data and threaten to make it publicly available.

 Solution

Having regular and complete backups of important data stored in a secure location is the best defense against ransomware attacks. A strong backup and recovery strategy reduces the attacker's leverage, enabling you to remove and restore the compromised data.

1.2. Remote Code Execution

An intruder will look for areas inside your application, such a search box, data entry field, or contact form, where users may enter information. The hacker then discovers what different requests and field content will accomplish by trial and error.

 Solution

Update any framework, content management system, or programming platform frequently with security updates. Observe input sanitization best practices when programming. All user input, regardless of how little, needs to be compared against a fundamental set of guidelines for what constitutes appropriate input.

1.3. Cross-Site Scripting (XSS)

Hackers that use XSS to target your clients typically utilize JavaScript and other browser-side scripting techniques to spread malware or unwanted adverts through your website. As a result, you risk losing the confidence of your customers and damaging your company's brand.

 Solution

Make changes to your content security policy. This simple but frequently missed step can stop a lot of XSS assaults before they ever start. The majority of XSS assaults rely on the site developer's lack of action to stop it. If you are a developer, you may utilize input sanitization to reduce these online security issues by correctly escaping HTML tag characters. For example, you can change < and > to < and > on any user input that JavaScript processes. Taking a few simple precautions can increase safety significantly.

1.4. Data Breach

Anytime an unauthorized person has access to your personal information, there has been a data breach. They may not be able to read or modify the data, but they do have access to a duplicate of it. You might not even be aware right away. For instance, the attacker could already know the password to the administrator account, but they haven't utilized it to make any modifications.

 Solution

At this point, an attacker is usually taking precautions to stay inconspicuous, which makes addressing this Internet security issue difficult. When you log in, a lot of systems will publish the connection details from your last session. When this information is accessible, take note of it and keep an eye out for unfamiliar activities.

1.5. Malware and Virus Infection

On a workstation, malware can track keystrokes to get passwords or encrypt data for ransomware purposes. Malware is often used by hackers to increase access to your website or provide access to others on the same network.

 Solution

Reduce the possibility of this security issue on workstations and personal devices by being cautious about what you download and by using antivirus software to detect and properly delete any malware. It's important to update these antivirus programs on a regular basis since malware is always evolving and getting better.

1.6. DDoS Attack

DoS (denial of service) attacks have a subclass known as distributed denial of service (DDoS) attacks. A distributed denial of service (DDoS) attack uses a network of interconnected computers, or "botnet," to flood a target website with fictitious traffic.

 Solution

The best defenses take all the traffic and absorb it by scaling up server and network resources to handle the extra load until the assault abates or can be contained.

2. Solution for public, private, hybrid, community ‘s cloud issues

2.1. Solution for Public

Intel-Driven Public Cloud Solutions Certain workloads are more appropriate for private infrastructure, while others are better suited for the public cloud. A hybrid, multicloud strategy will yield the greatest benefits for the majority of enterprises. In order to guarantee that you may utilize your desired combination of public and private cloud resources, Intel collaborates with ecosystem partners including VMWare - Intel Virtualize ASAP, Red Hat, and Microsoft in addition to leading cloud service providers (CSPs) like AWS, Google Cloud, and Microsoft Azure.

2.2. Solution for Private

Internal cloud, often known as private cloud, is a pre-installed system. It allows access to customer-specific resources, such as software and hardware. The firewall-protected system and the enterprise itself are the primary means of managing the model.

2.3. Solution for Hybrid

The answer to separating cloud infrastructure and data center transition is hybrid cloud. The Public Cloud, which is powered by Google Cloud, AWS, and cloud services combined on a single management engine, is then connected to this cloud architecture. From then, companies use a central control to assign, oversee, and manage resources.

2.4. Solution for Community

Because Community Cloud is adaptable and extendable, it works well for most users. Clients may personalize computers and smart mobile devices to suit their needs. therefore cutting expenses and the need for workers to interact remotely with clients. Lastly, Community Cloud guarantees trust and data security.

3. Methods to Ensure Security in the cloud

Now that the several concerns associated with cloud computing have been discussed, let's look at the solutions the industry has created to address these problems. In addition to briefly examining the tactics utilized to address the other secondary concerns, this part will concentrate on the techniques utilized to guarantee the distinct types of data security.

3.1. Countermeasures for Security Risks

We provide a brief summary of the several methods that are applied in the industry to secure specific problems in these domains.

 Organizational Security Risks

Malicious Insiders: Strict legal requirements should be included in employment contracts to reduce the possibility of having hostile employees within a CSP's workforce. Preventing this may also be greatly aided by a thorough third-party evaluation of the CSP and a strong security breach reporting procedure.

 Physical Security Risks

Physical Breach: Having robust physical security measures in place, such as armed guards, keycard access, and biometric scans to restrict access to sensitive locations in the data center, can help lower the risk of hackers physically accessing devices used in the provision of cloud services.

 Technological Security Risks

Virtualized defense and reputation-based trust management: CSP may employ a hierarchy of DHT-based overlay networks, with each layer responsible for carrying out particular functions. The lowest layer looks at colluders and handles reputation aggregation. The topmost layer handles several types of assaults. Interoperability and security through a trust model: Providers and users should have their own domains, each with a unique trust agent.

 Compliance and Audit Risks

Since this field mostly deals with legal matters, it is important for CSPs and CSCs to be aware of their legal and regulatory responsibilities and to make sure that any contracts they enter into comply with them. Additionally, the CSP needs to make sure that data security and privacy are not jeopardized by its discovery capabilities.