Vision of Cloud Computing

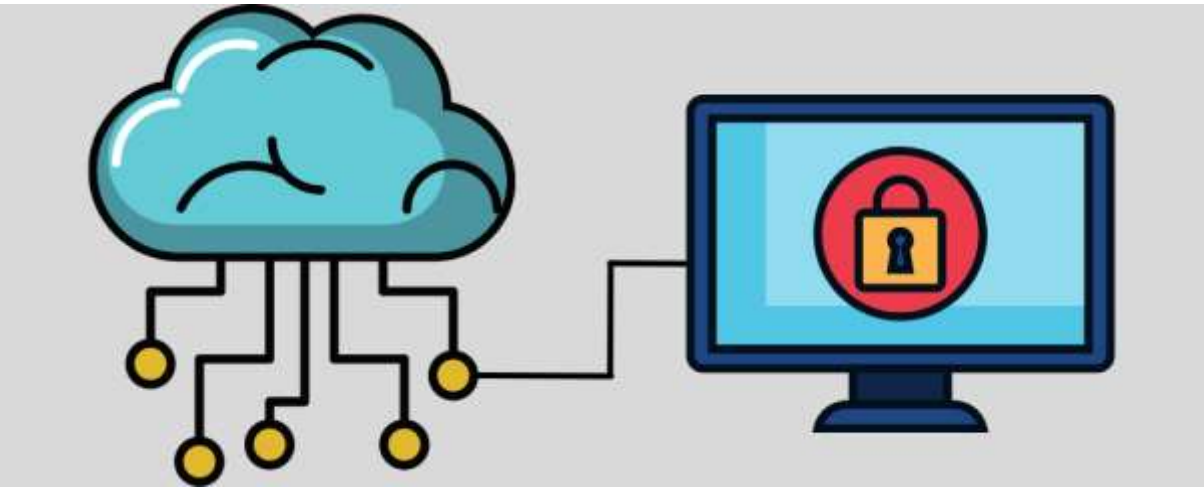
1. Cloud computing provides the facility to provision virtual hardware, runtime environment and services to a person having money.
2. These all things can be used as long as they are needed by the user.
3. The whole collection of computing system is transformed into collection of utilities, which can be provisioned and composed together to deploy systems in hours rather than days, with no maintenance cost.
4. The long term vision of a cloud computing is that IT services are traded as utilities in an open market without technological and legal barriers.
5. In the future, we can imagine that it will be possible to find the solution that matches with our requirements by simply entering out request in a global digital market that trades with cloud computing services.
6. The existence of such market will enable the automation of discovery process and its integration into its existing software systems.
7. Due to the existence of a global platform for trading cloud services will also help service providers to potentially increase their revenue.
8. A cloud provider can also become a consumer of a competition service in order to fulfill its promises to customers.
9. In the near future we can imagine a solution that suits our needs by simply applying our application to the global digital market for cloud computing services.
10. The presence of this market will enable the acquisition process to automatically integrate with its integration into its existing software applications. The availability of a global cloud trading platform will also help service providers to increase their revenue.
11. A cloud provider can also be a buyer of a competitive service to fulfill its promises to customers.

Risk and Challenges in Cloud Computing

#1. Data Security and Privacy

The biggest concern with cloud computing is data security and privacy. As organizations adopt the cloud on a global scale, the risks have become more grave than ever, with lots of consumer and business data available for hackers to breach.

According to Statista, 64% of respondents in a survey conducted in 2021 said data loss or leakage is their biggest challenge with cloud computing. Similarly, 62% said data privacy was their second most challenge.



The problem with cloud computing is that the user cannot view where their data is being processed or stored. And if it is not handled correctly during cloud management or implementation, risks can happen such as data theft, leaks, breaches, compromised credentials, hacked APIs, authentication breaches, account hijacking, etc.

How to prevent/minimize it: To ensure your data remains safe, find out if your cloud service provider has safe and secure identity authentication, management, and access controls. Ask them what sort of security they provide and against what factors. Do they have enough resources and expertise to handle the issues if something goes wrong? If you have a satisfactory answer to these questions, choose the cloud service provider.

#2. Compliance Risks

Compliance rules are getting more stringent due to the increased cyberattacks and data privacy issues. Regulatory bodies like HIPAA, GDPR, etc., ensure organizations comply with applicable state or federal rules and regulations to maintain data security and privacy for their business and customers.

However, compliance is another big challenge for organizations adopting the cloud. In the same survey by Statista, compliance is the third most significant challenge for 44% of respondents.

The issues arise for anyone using cloud storage or backup services. When organizations move their data from on-premises to the cloud, they must comply with the local laws. For example, every healthcare institution must comply with HIPAA in the US.

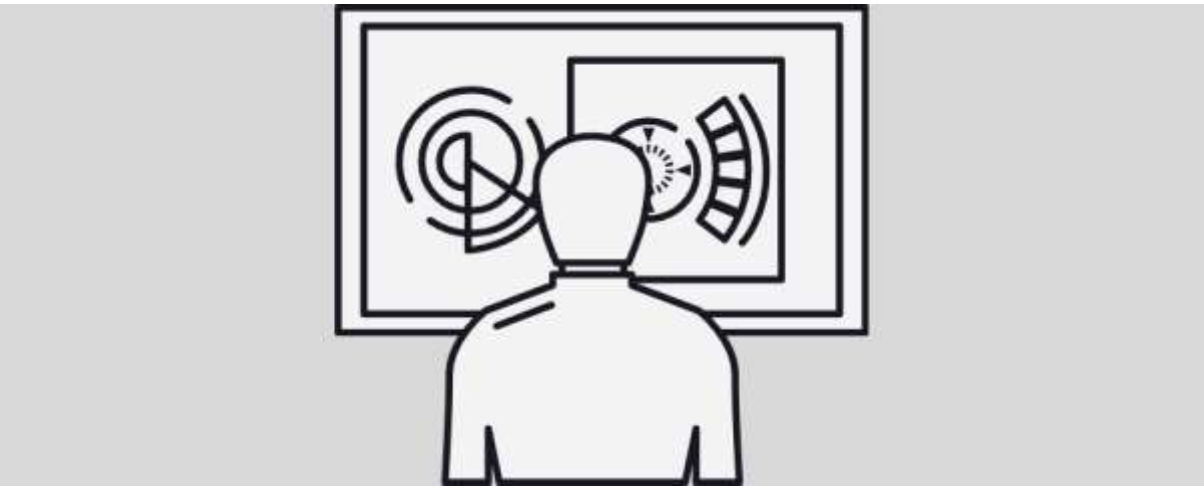
And if they don't do it by any means, they could face penalties that can tarnish their reputation and cost them money and customer trust.

How to prevent/minimize it: Choose the vendors that are compliant with the standards applicable in your state or country. Many cloud service providers can offer certified compliance, while for others, you may have to dig deeper and understand how and what regulations they are compliant with.

This will ensure that whatever cloud service you choose, you will be compliant with the laws applicable in your area. It not only saves you during audits and from penalties but also maintains customer trust.

#3. Reduced Visibility and Control

Cloud computing offers the benefit of not having to manage the infrastructure and resources like servers to keep the systems working. Although it saves time, expenses, and effort, the users end up having reduced control and visibility into their software, systems, applications, and computing assets.



As a result, organizations find it challenging to verify how efficient the security systems are due to no access to the data and security tools on the cloud platform. They also can't implement incident response because they don't have complete control over their cloud-based assets. In addition, organizations can't have complete insight into their services, data, and users to identify abnormal patterns that can lead to a breach.

How to prevent/minimize it: Before implementing the cloud, organizations must dig out all the necessary details about what data they can access, how to track it, and what security and controls the provider uses to mitigate risks and data breaches.

This will give you an overview of how much visibility and control you can expect from them. In addition, you can perform continuous monitoring and periodic analysis to get a better insight into your data, applications, users, and services. For this, there are many services providers you can find in the market.

#4. Cloud Migration

Cloud migration means moving your data, services, applications, systems, and other information or assets from on-premises (servers or desktops) to the cloud. This process enables computing capabilities to take place on the cloud infrastructure instead of on-premise devices.

When an organization wants to embrace the cloud, it can face many challenges while moving all its legacy or traditional systems to the cloud. The overall process can consume a lot of time, resources, and they have little idea how to deal with expert cloud providers already in business for years.

Similarly, when they want to migrate from one cloud provider to another, they have to do it all over again, and they are not sure how the next provider will serve them. They face challenges like extensive troubleshooting, speed, security, application downtime, complexity, expenses, and more. All these are troublesome for organizations and also for their users. Ultimately, it can lead to poor user experience and thus, affect organizations in various directions.

How to prevent/minimize it: Before you choose a cloud service provider, make sure to analyze your cloud requirements, security postures, and other areas that might get affected while migrating to the cloud. For this, you can compare different cloud service providers and determine which one can provide the best service to you, ensuring you get minimal trouble in business operations.

#5. Incompatibility

While moving your workload to the cloud from on-premises, incompatibility issues may arise between the cloud services and on-premises infrastructure.

This is a big challenge that may require the organizations to invest in making it compatible by any means or by creating a new service altogether. Either way, it invites troubles and expenditures for organizations.

How to prevent/minimize it: Before finalizing a cloud provider, make a list of all your services, assets, technologies, and systems you would like to move to the cloud. Now, ask your cloud provider about how compatible their services are with yours, and if it's a match, you can go for the service provider.

If most services are incompatible, you may move to the next service provider you have shortlisted and repeat the same process to find the best one suitable for your needs.

#6. Improper Access Controls and Management

Improper or inadequate cloud access controls and management can lead to various risks for an organization. Cybercriminals leverage web apps, steal credentials, perform data breaches, and whatnot. They may face access management issues if they have a large or distributed workforce.

In addition, organizations can also face password fatigue and other issues such as inactive users signed for long terms, poorly protected credentials, weak passwords, multiple admin accounts, mismanagement of passwords, certificates, and keys, and more.

As a result of poor access controls and management, organizations can be vulnerable to attacks. And their business information and user data can be exposed. Ultimately, it can cause reputation damage and increase unnecessary expenses.

How to prevent/minimize it: Organizations must have proper data control and management for their user accounts to avoid such issues. All those accounts must be securely linked with a central governing authority to administer who is accessing what systems.

There are many identity and access providers available whose help you can ensure only authorized personnel can access your network, systems, and applications. You can use a third-party or cloud-native tool to analyze all the users, groups, and roles. The IAM solutions can show you who has access to information and resources. It will also help you detect suspicious activities and take immediate actions to stay protected.

#7. Lack of Expertise

Cloud technologies are rapidly advancing, and more and more services and applications are being released to cater to different needs. However, it's also becoming difficult for organizations to find skilled professionals to maintain the cloud systems. It's also costly for small and medium-sized businesses to hire expert cloud professionals.

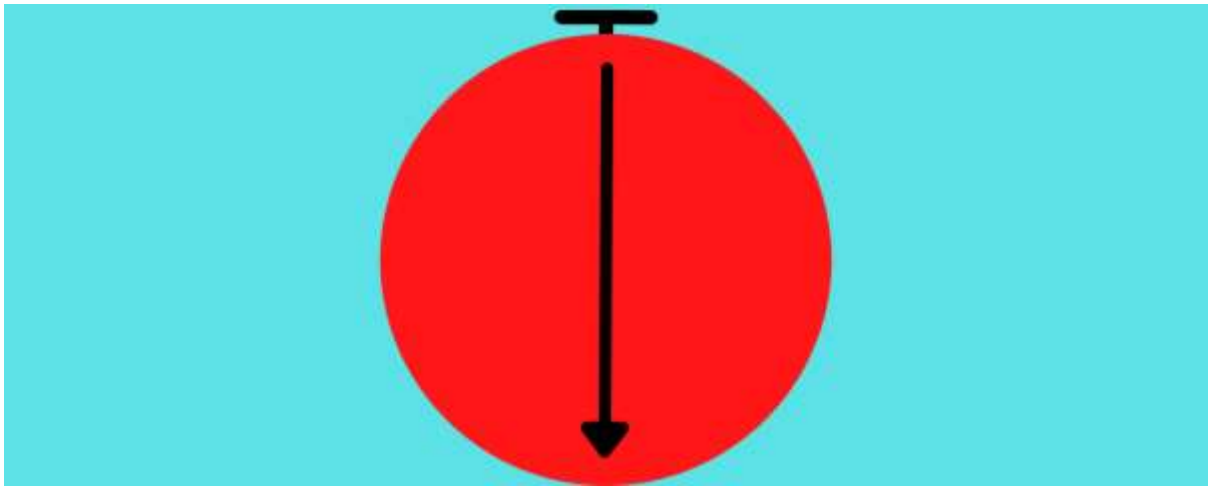
The reason is the cloud is a new concept for many, and it's still not mainstream. Not everyone in your team will be familiar with cloud technologies. And hence, your IT staff must also be trained how to use the cloud technologies efficiently by themselves. It again incurs a high cost, which is a burden for organizations with a limited budget. They will have to pay for the instructor and invest in recruiting and onboarding cloud professionals.

How to prevent/minimize it: Organizations adopting new cloud technologies must ensure they are using technologies that are easy to use, implement, and deploy, with not so steep learning curves. You must also run in-house training where your senior cloud professionals can train the new or other staff for cloud technologies.

#8. Downtime

Another irritating thing about the cloud for many organizations can be downtime due to poor internet connection.

If you have a consistent and high-speed internet connection, you can make the most of their cloud services. But if you don't, you may face repeated downtimes, lags, and errors. It not only frustrates the users but also reduces their productivity.



This way, organizations with poor internet connectivity are likely to face disruption in their business operations. They won't be able to access their data whenever they want. Hence, they can meet a lot of inefficiencies, missed deadlines, and whatnot. All these can invite bottlenecks for business operations and lead to reduced sales, revenue, and profit margins.

How to prevent/minimize it: Organizations adopting cloud technologies must ensure they have consistent and quality internet connectivity. If not, they must invest more to get that speed and uptime they need to access their systems and technologies whenever they require constantly. It will increase their productivity and work efficiencies and reduce security issues that may sleep in during downtimes.

#9. Insecure APIs

Using application interfaces APIs in cloud infrastructure enables you to implement better controls for your systems and applications. They are either in-built into the mobile apps or web to allow the employees and users to access the systems.

However, if the external APIs you use are insecure, it can invite a lot of trouble for you in terms of security. These issues can provide an entry point for attackers to hack into your confidential data, manipulate services, and do other harm.

Insecure APIs can cause broken authentication, security misconfigurations, break function-level authorization, expose data, and mismanagement of resources and assets.

How to prevent/minimize it: You must ensure that your developers design APIs with robust access control, encryption, and authentication protocols in order to avoid this issue. It will provide you with a secure, reliable, and powerful API that hackers can't leverage easily.

In addition, you can run penetration testing to find vulnerabilities and fix them before they cause any issues. You can also implement TLS/SSL encryption for data transfer and execute multi-factor authentication using digital identities, biometrics, OTPs, and other strong identity and access management techniques.

So, the above were the risks and challenges you might face while implementing cloud computing. But there are ways to prevent or minimize those troubles, as discussed above.