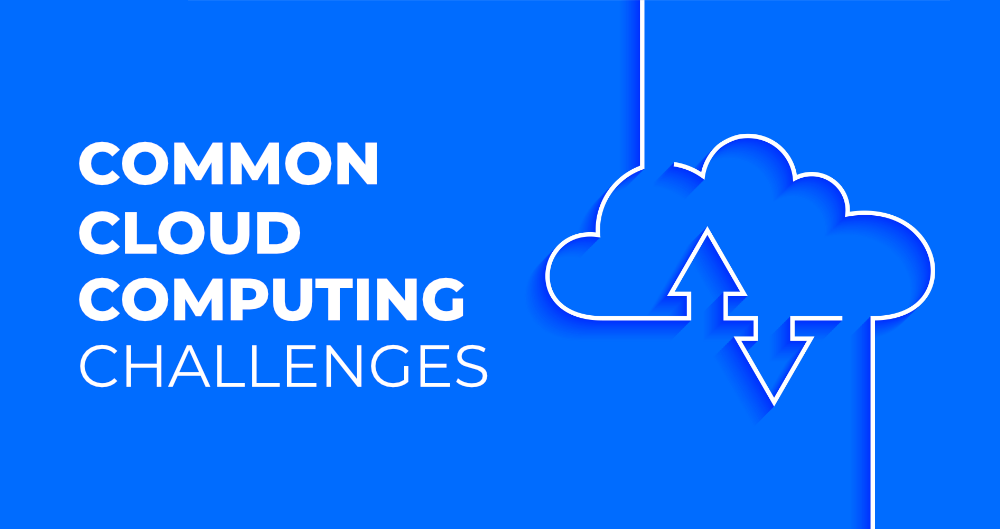
**Cloud Computing Challenges**

Cloud computing is the provisioning of resources like data and storage on demand, that is in real-time. It has been proven to be revolutionary in the IT industry with the market valuation growing at a rapid rate. Cloud development has proved to be beneficial not only for huge public and private enterprises but small-scale businesses as well as it helps to cut costs. It is estimated that more than 94% of businesses will increase their spending on the cloud by more than 45%. This also has resulted in more and high-paying jobs if you are a cloud developer.



Cloud technology was flourishing before the pandemic, but there has been a sudden spike in cloud deployment and usage during the lockdown. The tremendous growth can be linked to the fact that classes have been shifted online, virtual office meetings are happening on video calling platforms, conferences are taking place virtually as well as on-demand streaming apps have a huge audience. All this is made possible by us of [**cloud computing**](https://www.geeksforgeeks.org/cloud-computing/) only. We are safe to conclude that the cloud is an important part of our life today, even if we are an enterprise, student, developer, or anyone else and are heavily dependent on it. But with this dependence, it is also important for us to look at the issues and challenges that arise with cloud computing. Therefore, today we bring you the most common challenges that are faced when dealing with cloud computing, let’s have a look at them one by one:

**1. Data Security and Privacy**

Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control. Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications. This can in turn lead to potential loss in revenue alongside reputation and stature. Also, dealing with cloud computing requires sending and receiving huge amounts of data at high speed, and therefore is susceptible to data leaks.

**2. Cost Management**

Even as almost all cloud service providers have a “Pay As You Go” model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing. When there is under optimization of the resources, let’s say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up. If you turn on the services or an instance of cloud and forget to turn it off during the weekend or when there is no current use of it, it will increase the cost without even using the resources.

**3. Multi-Cloud Environments**

Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team. The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.

**4. Performance Challenges**

Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits. Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience. Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

**5. Interoperability and Flexibility**

 When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since applications written for one cloud with the application stack are required to be re-written for the other cloud. There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues encountered when changing cloud solutions, thereby reducing flexibility.

**6. High Dependence on Network**

Since cloud computing deals with provisioning resources in real-time, it deals with enormous amounts of data transfer to and from the servers. This is only made possible due to the availability of the high-speed network. Although these data and resources are exchanged over the network, this can prove to be highly vulnerable in case of limited bandwidth or cases when there is a sudden outage. Even when the enterprises can cut their hardware costs, they need to ensure that the internet bandwidth is high as well there are zero network outages, or else it can result in a potential business loss. It is therefore a major challenge for smaller enterprises that have to maintain network bandwidth that comes with a high cost.

**7. Lack of Knowledge and Expertise**

Due to the complex nature and the high demand for research working with the cloud often ends up being a highly tedious task. It requires immense knowledge and wide expertise on the subject. Although there are a lot of professionals in the field they need to constantly update themselves. Cloud computing is a highly paid job due to the extensive gap between demand and supply. There are a lot of vacancies but very few talented cloud engineers, developers, and professionals. Therefore, there is a need for upskilling so these professionals can actively understand, manage and develop cloud-based applications with minimum issues and maximum reliability.

**Risk of cloud computing**

### 2. Limited Visibility Into Network Operations

When businesses use a mix of cloud platforms and environments as well as on-premises servers, this infrastructure can become complex and cause limited visibility within a network. Although complex networks can cause inefficient operations and network downtime, leading to overspending, the main security issue is the unintentional creation of network “dark spots.” This term refers to areas within a cloud network or infrastructure that monitoring tools frequently miss, leaving those segments open and exposed to a security breach.

Managing a network incorrectly equates to waving a welcome sign to all potential hackers as [cybercriminals can use automated tools](https://builtin.com/artificial-intelligence/why-we-cant-ignore-dark-side-ai) to scan for vulnerabilities in cloud applications, servers, and infrastructure, leading to security breaches. Worse, businesses often won’t realize they’ve been breached in real time due to network darkness, leading to significant data loss and remediation costs.

### 3. Compliance Issues

The [regulations you have to comply with](https://builtin.com/tag/compliance) depend on your industry or the service you provide. Two of the most widespread and relevant pieces of legislation regarding cloud computing are the EU General Data Protection Regulation (GDPR) and the [Health Insurance Portability and Accountability Act of 1996 (HIPAA)](https://builtin.com/healthcare-technology/phi-protected-health-information).

Issues surrounding compliance can occur when companies don’t abide by the principle of least privilege (PoLP) or are following several [compliance regulations](https://builtin.com/cybersecurity/data-compliance-close-more-deals) simultaneously, causing overlap or ambiguity on how they should keep information. Breaking compliance laws can result in hefty fines and legal fees for the guilty parties.

### 4. Data Loss

Although one of the major reasons to use cloud computing is to safeguard data and assets, it is not immune to data loss.

One significant cause of data loss is insufficient data backup and recovery. Many startup owners and entrepreneurs place too much faith in the cloud, meaning they don’t have adequate planning and resources for data recovery. In the event of physical damage, [cyber attacks](https://builtin.com/cybersecurity/types-of-cyber-attacks" \t "_blank) or insider threats, data can be permanently lost if regular backups and contingency plans are not in place.

More on Cloud Computing[How Combining Observability With Edge Computing Ensures Greater Productivity](https://builtin.com/cloud-computing/combining-observability-edge-computing)

### 5. Data Breaches

Surprisingly, or perhaps not, the largest cause of [data breaches](https://builtin.com/cybersecurity/cybersecurity-investment) is human error. According to Verizon’s 2023 Data Breaches Investigations Report, [74 percent](https://www.verizon.com/business/resources/reports/dbir/) of data breaches involved a human element, whether intentional or not.

Furthermore, the number one cause of human data breaches is [weak or stolen credentials](https://builtin.com/cybersecurity/data-breach-password). A survey from [GoodFirms](https://www.goodfirms.co/resources/top-password-strengths-and-vulnerabilities" \t "_blank), which questioned IT experts and cybersecurity personnel, found that 30 percent of respondents had experienced a data breach due to weak credentials, 36 percent write their passwords down on paper, and 53 percent share their passwords with colleagues, family and friends. All of these practices are a recipe for a breach.

So, non-IT employees can’t take all the blame regarding data breaches when some IT professionals don’t even follow their own cybersecurity protocols.

### 6. Account Hijacking

This won’t be news to you but, if users write down their cloud account password or share it with others, the chance of their cloud accounts being hijacked increases. As a result of this type of negligence, hackers can gain access to employees’ emails and, from there, can easily access their whole cloud accounts.

Account hijacking is particularly attractive to cybercriminals since [33 percent](https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf) of all company folders are open to everyone, and it’s made even easier when mixed with network visibility weak spots and poorly chosen passwords. Therefore, cybercriminals can hijack accounts easily and find valuable data readily available even on entry-level employee accounts.