**Disadvantages of cloud computing**

**- Deepthi Tabitha Bennet (20S009) & Preethi Samantha Bennet (20S026)**

**1). Downtime**

Downtime is often cited as one of the biggest cloud computing disadvantages. Since cloud computing systems are internet-based, service outages are always an unfortunate possibility and can occur for any reason.

The financial impact of service disruptions and outages is staggering. A recent survey conducted by [Uptime Institute](https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/AnnualOutageAnalysis2023.03092023.pdf?mkt_tok=NzExLVJJQS0xNDUAAAGKjSDFvBZwbOB6fZpkNV3lXIyqC1Xo_fMcQCiK_HKyPKNwNPy6Gpj6voIWChuo_sCejR_L8bhFNDxeRne05FDAnt-uG-sgRb2-WtoiDDT7Jw) indicates that about 31% of businesses have experienced an IT service incident or outage that significantly impacted their operations within the past three years. On average, an outage and or slowdown can cost a business upwards of $100,000 an hour. Unfortunately, no organization is immune, especially when critical business processes cannot afford to be interrupted. In 2023 several companies and services were [hit by outages](https://www.crn.com/news/cloud/the-10-biggest-cloud-outages-of-2023-so-far-#:~:text=Cloud%20Outages%20In%202023&text=Cloud%20downtime%20can%20cost%20users,hit%20%24591.8%20billion%20this%20year.), including IT Glue, Microsoft, Google Cloud and AWS, Oracle, and Datadog.

Minimizing planned downtime in a cloud environment

* Design services with high availability and disaster recovery in mind. Leverage the multi-availability zones provided by cloud vendors in your infrastructure.
* If your services have a low tolerance for failure, consider multi-region deployments with automated failover.
* Define and implement a disaster recovery plan that provides the lowest recovery time (RTO) and recovery point objectives (RPO).
* Consider implementing dedicated connectivity such as AWS Direct Connect, Azure ExpressRoute, or Google Cloud’s Dedicated Interconnect or Partner Interconnect. These services provide a dedicated network connection between you and the cloud service point of presence. This can reduce exposure to the risk of business interruption from the public internet.
* Read the fine print on your Service Level Agreement (SLA). Are you guaranteed 99.9% uptime or even better? That 0.1% downtime equals about 45 minutes per month or around eight hours per year.

**2). Security and privacy**

Although cloud service providers implement the best security standards and industry certifications, storing data and important files on external service providers always opens up risks. Any discussion involving data must address security and privacy, especially when it comes to managing sensitive data. We must not forget what happened at [Code Space](https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html) and the hacking of their AWS EC2 console, which led to data deletion and the eventual shutdown of the company. Their dependence on the remote cloud meant the risk of outsourcing everything.

Of course, any cloud computing service provider is expected to manage and safeguard the underlying hardware infrastructure of a deployment. However, your responsibilities lie in the realm of user access management, and it’s up to you to carefully weigh all the risk scenarios.

Though recent breaches of credit card data and user login credentials are still fresh in the minds of the public, steps have been taken to ensure the safety of data. One such example is the [General Data Protection Rule (GDPR),](https://cloudacademy.com/4-best-practices-to-get-your-cloud-deployments-gdpr-ready/) which was recently enacted in the European Union to provide users more control over their data.

Minimizing security and privacy risks

* Understand the [shared responsibility model](https://cloudacademy.com/aws-shared-responsibility-model-security/) of your cloud provider. You will still be liable for what occurs within your network and in your product.
* [Implement security](https://cloudacademy.com/whitepapers/architecting-security-first-into-cloud-strategy/) at every level of your deployment.
* Know who is supposed to have access to each resource and service, and limit access to least privilege. If an employee goes rogue and gains access to your deployment, you would want their impact to be over the smallest area as possible.
* Make sure your team’s skills are up to the task. The [Top 10 Things Cybersecurity Professionals Need to Know](https://cloudacademy.com/blog/top-things-cybersecurity-professionals-need-to-know/) is a great article to understand how to mitigate security and privacy concerns in the cloud.
* Take a risk-based approach to securing assets and extend security to the devices.
* Implement multi-factor authentication for accounts accessing data/ systems.
* Turn on encryption wherever you can — easy wins are on object storage such as Amazon S3 or Azure Blob Storage where customer data often resides. The simple act of turning on encryption on S3 could have prevented the [Capital One data breach](https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html) in July 2019 that exposed 100 million users’ information.

**3). Limited control and flexibility**

Since the cloud infrastructure is entirely owned, managed, and monitored by the cloud service provider, it transfers minimal control over to the customer.

To varying degrees (depending on the particular service), cloud users may find they have less control over the function and execution of services within a cloud-hosted infrastructure. A cloud provider’s end-user license agreement (EULA) and management policies might impose limits on what customers can do with their deployments. Customers retain control of their applications, data, and services, but may not have the same level of control over their backend infrastructure.

Maintaining control and flexibility

* Consider using a cloud service provider partner to help with implementing, running, and supporting cloud services.
* Understand your responsibilities and the responsibilities of the cloud vendor in the shared responsibility model to reduce the chance of omission or error.
* Make time to understand your cloud service provider’s basic level of support. Will this service level meet your support requirements? Most cloud service providers offer additional support tiers above the basic support for an additional cost.
* Make sure you understand the SLA concerning the infrastructure and services you’re going to use and how that’ll impact your agreements with your customers.

**4). Vendor lock-in**

Vendor lock-in is another perceived disadvantage of cloud computing. Easy switching between cloud services is a service that hasn’t yet completely evolved, and organizations may find it difficult to migrate their services from one vendor to another. Differences between vendor platforms may create difficulties in migrating from one cloud platform to another, which could equate to additional costs and configuration complexities. Gaps or compromises made during migration could also expose your data to additional security and privacy vulnerabilities.

Decreasing dependency

* Design with cloud architecture best practices in mind. All cloud computing services provide the opportunity to improve availability and performance, decouple layers, and reduce performance bottlenecks. If you have built your services using cloud architecture best practices, you are less likely to have issues porting from one cloud platform to another.
* Properly understand what your vendors are selling to avoid lock-in challenges.
* Employ a multi-cloud strategy to avoid vendor lock-in. While this may add both development and operational complexity to your deployments, it doesn’t have to be a deal breaker. Training can help prepare teams to [architect and select best-fit services and technologies](https://cloudacademy.com/solutions/manage-the-multi-cloud/).
* [Build in flexibility](https://cloudacademy.com/separating-multi-cloud-strategy-from-hype-whitepaper/) as a matter of strategy when designing applications to ensure portability now and in the future.
* Build your applications with services that offer cloud-first advantages, such as modularity/ portability of microservices. Think containers and Kubernetes.

**5). Cost concerns**

The last one of the disadvantages of cloud computing concerns cost. Adopting cloud solutions on a small scale and for short-term projects can be perceived as being expensive. However, the most significant cloud computing benefit is in terms of IT cost savings. Pay-as-you-go cloud services can provide more flexibility and lower hardware costs, but the overall price tag could end up being higher than you expected. Until you are sure of what will work best for you, it’s a good idea to experiment with a variety of offerings.

Reducing costs

* Try not to over provision your services, but rather use auto-scaling services.
* Ensure you have the option to scale DOWN as well as UP.
* Pre-pay and take advantage of reserved instances if you know minimum usage.
* Automate the process to start/stop your instances to save money.
* Create alerts to track cloud spending.