Challenges of Cloud Computing

Cloud service refers to the collection of policies, procedures, controls and technologies, that work together to shield and cushion cloud based systems, data and infrastructures. It is essential for organizations to implement cloud security tools and services, in order to address internal and external threats within the business. The potentiality of cloud security is to safeguard company's leaks, accidental data loss and other valuable assets. Diving deep into cloud security, there are a total of three major cloud environments. They are:

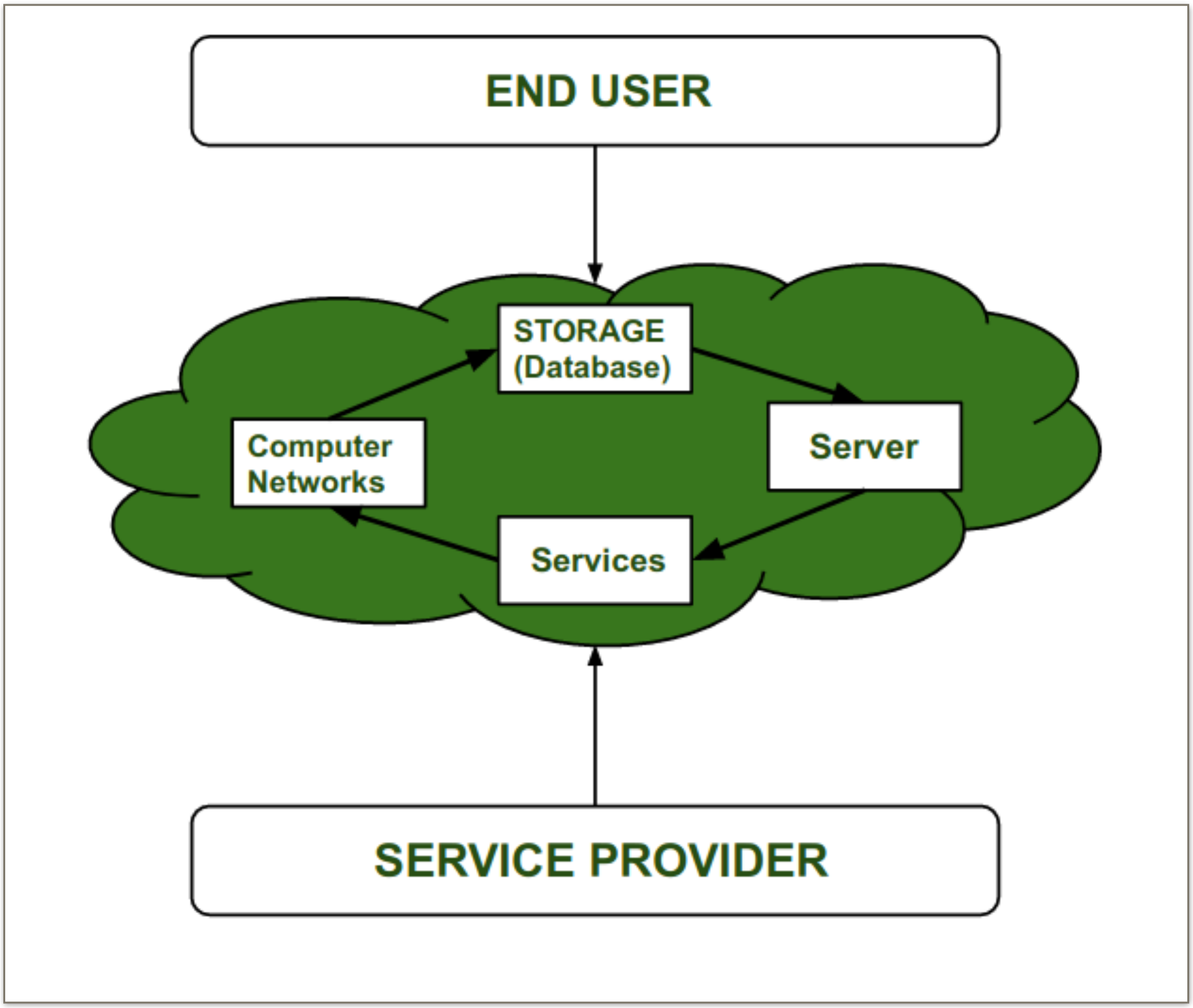

Fig. : Diagrammatic representation of Cloud Computing

Cloud Environments	Description
Public Clouds	Hosted by third-party cloud service providers where providers handle everything including setup
Private Clouds	More secured than public clouds which focus single group of user, relying on its firewall
Hybrid Clouds	Combination of both public and private clouds which can be scaled on user's demand

Cloud security has plenty of advantages, especially for organizations who are focused on securing their cloud data from any sort of unauthorized access. This includes reducing costs, easy scaling, and many more security upgrades (The Biggest Cloud Security Challenges in 2021, 2022). However, there are handful of challenges regarding cloud security as well. Some of them are :

1. **Data Loss and Breaches :**

The main reason to implement data security tools is to safeguard crucial data. If a company fails to protect data despite having close security measures, then there is no value of it. Data breaches can cause some serious damages to a company, including social reputation and legal responsibilities.

2. **Data Confidentiality :**

Organizations have a large amount of internal data that is essential to maintaining competitive advantage. Most of these data are stored in cloud by respective companies. However there are issues with confidentiality and security of data. This might make organization face legal issues, paying millions of rupees as fines.

3. **Misconfigurations :**

If data and resources are configured inappropriately, chances of data violation can increase significantly. There are possibilities of unauthorized users breaching data and valuable information from loopholes created during misconfigurations. Therefore, this vulnerability of insecure storage can be minimized by observing viewers access in internet carefully.

4. IAM Issues

IAM stands for ‘Identity and Access Management’, which is a business process framework that helps to keep digital identities secured. IAM uses security systems such as two-factor authentication and sign-on systems. Despite all these, there are security issues in IAM because of weak passcodes, scalability changes and improper credentials (Gittlen & Rosencrance, 2021).

5. Insecure Interfaces and API

APIs through which customer interact with cloud services are one of the most vulnerable gateway for data contravention. A hacker or any user with cloud accessing knowledge can authorize into an organization’s data through API as well. Therefore, it is crucial that reuse of API must be avoided and API hygiene must be maintained by designing, developing, testing and deploying according to standard laws ("Top 11 cloud security challenges and how to combat them", 2022).

References

The Biggest Cloud Security Challenges in 2021. (2022, May 11). Check Point Software. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-native-security/the-biggest-cloud-security-challenges-in-2021/

Gittlen, S., & Rosencrance, L. (2021, August 10). *What is identity and access management? Guide to IAM*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Dosal, E. (2020, March 5). *7 Cloud Security Challenges and Risks to Be Aware Of*. COMPUQUIP. https://www.compuquip.com/blog/cloud-security-challenges-and-risks