International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cloud Computing

Ms. Sumandeep Kaur

Asst. Prof. in Computer Science Deptt Govind National College Narangwal Ldh

Abstract:
Cloud computing might seem like another new technology to anyone looking at it for the first time. But cloud computing is like old wine in new bottle. Cloud Computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs and just-in-time availability of resources. Cloud Computing is a technology that allows you to store and access data and applications over the internet instead of using your computer's hard drive or a local server. At the present time the demand for cloud computing services are increasing with respect to that demand for cloud computing skills is also increasing. This paper provides the brief information about the cloud computing, its security issues and what is to be done to remove the security threats.

Keywords: Visualization, Encryption, platform, authorization, protection.

INTRODUCTION

The term "cloud computing" was first used by computer scientist Ramnath Chellappa in a paper published in 1997, in which he described the emerging paradigm of delivering computing services over the internet. However, it was not until the mid-2000s, with the rise of virtualization and the development of web services, that cloud computing began to take off as a commercial concept. Other early cloud providers included Google Cloud Platform (GCP) and Microsoft Azure, which both launched in 2008. Since then, cloud computing become mainstream for every business. Cloud computing is the on-demand availability of computing resources (such as storage and infrastructure), as services over the internet. It eliminates the need for individuals and businesses to self-manage physical resources themselves, and only pay for what they use. It provide the illusion of infinite computing resources are available on demand. It starts with storage but further it includes infrastructure, apps, platform and computation.

NEED OF CLOUD COMPUTING

The company had to buy powerful physical servers, storage disks, and networking equipment. This required a huge upfront investment, known as Capital Expenditure (CapEx). They had to guess their peak traffic needs, often buying far more capacity than they used day-to-day, leading to wasted resources. If they needed a new server, the process of ordering, installing, and configuring it could take weeks or even months. This is called the "old way" (**On-Premises).** The cloud changes this model entirely. Instead of buying hardware, you rent computing power from a cloud provider (like AWS, Google, or Microsoft). This shifts the cost from a large upfront investment to a manageable monthly bill, known as an Operational Expenditure (OpEx). This model eliminates guesswork, long waiting times, and wasted resources. This is called The "New Way" (Cloud Computing).

BENEFITS OF CLOUD-BASED COMPUTING

1. **Scalability:-**Cloud services are designed to be scalable, which means cloud's inherent ability to dynamically adjust computing resources(CPU, Storage, Network) to match fluctuating demands. Scalability is important because an organisation's cloud workload is not constant. Therefore, a scalable cloud environment should also provide predictable and consistent costs as workload change.
2. **Security:-** According to certain reports, small **private companies** are multiple times more likely to suffer a cyberattack than large organizations. That most likely shocks numerous owners of companies. As Cloud computing is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks
3. **Accessible to modern technology: -**Cloud computing is far more than an internet-based storage service for data. Organizations worldwide currently use cutting-edge technologies they need to get done with their responsibilities and run their business over the web utilizing the cloud. Some technology available on a cloud platform includes Artificial Intelligence and Machine Learning, Data Analytics, Data Visualization, Containerization, etc. The opportunity to build powerful AI applications and machine learning models without buying actual physical servers is a strong motivation.
4. **Cheaper: -**The cloud computing model is based on the '**pay-as-you-go'** principle and offers a possibly less expensive way for organizations to remain coordinated and online. Albeit the costs for hard drives, strong state drives, servers, and other fundamental things have fallen lately, cloud computing proves to be the best regarding cost expenses.
5. **Flexiblility: -**Due to the architecture of cloud computing, enterprises and their users can access cloud services from anywhere with an internet connection, scaling services up or down as needed. Cloud computing flexibility means the ability to instantly adjust IT resources without big hardware investments ensuring efficiency and agility.

loud computing also offers energy saving benefits attracting service providers to offer outsourcing solutions (Weissberger, 2011). Efficiency, scalability and flexibility makes cloud computing perfect for outsourcing sector which attracts organizations and individuals to outsource their services to cloud computing vendors (Stevens, 2009). Cloud computing meets organizations' and individuals' computing needs quickly where they can see improved efficiencies compared to traditional computing. Cloud computing offers better opportunity to focus on innovation for product growth which is more beneficial than traditional computing loud computing also offers energy saving benefits attracting service providers to offer outsourcing solutions (Weissberger, 2011). Efficiency, scalability and flexibility makes cloud computing perfect for outsourcing sector which attracts organizations and individuals to outsource their services to cloud computing vendors (Stevens, 2009). Cloud computing meets organizations' and individuals' computing needs quickly where they can see improved efficiencies compared to traditional computing. Cloud computing offers better opportunity to focus on innovation for product growth which is more beneficial than traditional computing Cloud computing also offers energy saving benefits attracting service providers to offer outsourcing solutions (Weissberger, 2011). Efficiency, scalability and

flexibility makes cloud computing perfect for outsourcing sector which attracts organizations and individuals to outsource their services to cloud computing vendors (Stevens, 2009). Cloud computing meets organizations' and individuals' computing needs quickly where they can see improved efficiencies compared to traditional computing. Cloud computing offers better opportunity to focus on innovation for product growth which is more beneficial than traditional computin

COMPONENTS OF CLOUD COMPUTING

1. **Application**

A cloud application influences **The Cloud** model of software architecture, often eliminating the need to install and run the application on the customer's own computer, thus reducing software maintenance, ongoing operations, and support. For example:

- Peer-to-peer/volunteer computing (Bittorrent, SETI@home, Skype)
- Web application (Facebook)
- Software as a service (Google Apps, Salesforce)
- Software plus services (Microsoft Online Services)

2. **Infrastructure**

Cloud infrastructure (e.g. Infrastructure as a service) is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. For example:

- Full virtualization (GoGrid, Skytap)
- Grid computing (Sun Grid)
- Management (RightScale)
- Paravirtualization (Amazon Elastic Compute Cloud)

3. **Platform**

A cloud platform (e.g. Platform as a service) (the delivery of a computing platform and/or solution stack as a service) facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. For example:

- Web application frameworks
- Python Django (Google App Engine)
- Ruby on Rails (Heroku)
- Web hosting (Mosso)
- Proprietary (Azure, Force.com)

4. **Service**

A cloud service (e.g. Web Service) is "software system designed to support interoperable machine-to-machine interaction over a network" which may be accessed by other cloud computing components, software (e.g. Software plus services) or end users directly. For example:

- Identity (OAuth, OpenID)
- Integration (Amazon Simple Queue Service)
- Mapping (Google Maps, Yahoo! Maps)
- Payments (Amazon Flexible Payments Service, Google Checkout, PayPal)
- Search (Alexa, Google Custom Search, Yahoo! BOSS)
- Others (Amazon Mechanical Turk)

5. **Storage**

Cloud storage is the delivery of data storage as a service (including database-like services), often billed

on a utility computing basis (e.g. per gigabyte per month). For example:

- Database (Amazon SimpleDB, Google App Engine's BigTable datastore)
- Network attached storage (MobileMe iDisk component, Nirvanix CloudNAS)
- Synchronisation (Live Mesh Live Desktop component, MobileMe push functions)
- Web service (Amazon Simple Storage Service, Nirvanix SDN)

6. **Artificial Intelligence**

Artificial Intelligence refers to (AI as a service) cloud based platform that offers ready- to-use AI tools and services enabling business to implement artificial intelligence without needing to build or maintaining the underlying infrastructure. Major Ai tools that integrate major AI technologies are:

- AWS Sage Maker, Amazon Rekognition , Amazon Polly, etc.
- Google Cloud Ai: Auto Ml, Vision AI, Dialogflow
- Microsoft Azure Ai: Azure cognitive services, Bot Framework, Azure Machine Learning.
- IBM Watson AI: Watson Assistant, Watson Discovery, Watson Natural Languages understanding.

CLOUD SECURITY THREATS AND MITIGATION STRATEGIES:

Data Security and privacy is the major challenge for the cloud providers as data is the most important assets of an organisation . Thus now we discuss some major security threats and mitigation strategies i.e. how to reduce or permanently remove the impacts of threats.

1. **Data Breaches:** A data breach can result in unauthorized access, theft, or exposure of sensitive information, leading to severe financial and reputational consequences.

Real Life examples:

Capital One(2019) -A misconfigured firewall led to the exposure of 100 million customers records, including bank details and social security numbers.

Mitigation strategies:

- **Data Encryption** : Encrypt sensitive data both at rest(i.e. store at server)and in transit.
- **Access Control :**Implement role based access control (RBAC) to data access. Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control.
- **Regular Security Audits**: Conduct periodic checking (i.e. what is accessed ,for how long accessing is done and who is the authoriser) to identity and fix vulnerabilities.

2. **Account Hijacking :**Cloud account hijacking is when attackers steal access to cloud services (like AWS, Google Cloud) by stealing credentials (phishing, malware) or exploiting vulnerabilities, allowing them to steal data, disrupt services, or launch further attacks, often using stolen credentials via phishing, malware, or credential stuffing.

Real Life examples:

Tesla's AWS Account Hack(2018) -Attackers gained access Tesla's AWS cloud account due to a poorly secured Kubernetes console.

Mitigation Strategies:

- Multi-Factor Authentication(MFA)Always enable MFA to add
- an extra layer of security.(eg two step verification in Gmail).
- 2.Least Privilege Principle: Limit account permissions to only what's necessary. means Give privilege to those who is actually required ie based on the work not on personal attachment.

- Continue Monitoring: Use SIEM(Security Information and Event Management) tools to detect suspicious activities.

3. **Insider Threats:** An insider threat in cloud computing is a security risk from someone within the organization (employee, contractor, partner) who misuses their authorized access to harm cloud systems, data, or infrastructure, either maliciously (theft, sabotage) or unintentionally (negligence, accidents like phishing)

Real Life Example: Amazon Web Services(AWS) Employee Leak(2020)-A former AWS employee misused customer data by exploiting internal access to cloud services.

Mitigation Strategies:

- User Activity Monitoring Log and monitor all user actions using CloudTrail(AWS) or Azure Monitor
- Strict Offboarding Process: Revoke access immediately when employees leave.
- Data Loss Prevention(DLP): implements DLP policies to prevent unauthorised data transfers.

4. **InSecure APIs:** Mostly cloud services are accessed through APIs. Because APIs work as the backend framework for systems and services, it's critical to secure APIs to protect the sensitive data they transfer — including access information, such as authentication, authorization, input validation and encryption. API security refers to the methods and tools designed to protect these backend frameworks and mitigate attacks from access violations, bot attacks and abuse.

Real Life Examples: Facebook API Data Leak (2019) - Misconfigured APIs exposed 540 million Facebook user records Amazon S3 Buckets(where majorly data is stored)

Mitigation Strategies:

- API Authentication: Use OAuth2.0 or JWTtokens to secure API access.
- Rate Limiting: Restrict the number of API requests to prevent abuse.
- Regular API Security Testing: Scan for vulnerabilities using OWASP API Security Testing.

5. **Distributed Denial Of Service (DDoS)Attacks**: DDoS (distributed denial-of-service attack) is an attempt at rendering a server unreachable to its visitors. During a DDoS attack your website may become unreachable since the server is being flooded with bogus requests and cannot process the valid ones

Real Life Example:

GitHub DDoS Attack(2018) : A record breaking 1.3 Tbps DDoS attacktargeted GitHub , disrupting services for 15-20 minutes.

Mitigation Strategies:

- DDoS Protection Service :Use AWS Shield ,Cloudflare or Azure DDoS Protecting.
- 2.Traffic Filtering :Deploy firewalls and load balancers to block malicious traffic
- 3.Auto-Scaling : Set up auto scaling in cloud infrastructure to handle high traffic

6. **Lack of Cloud Security Monitoring:** A lack of cloud security monitoring leaves organizations blind to threats, leading to misconfigurations, unauthorized access, data breaches, and compliance failures, stemming from complex.If security logs are not monitored, threats go undetected until a major attack occurs.

Real-Life Example:

Marriot Data Btrach(2018) - Attackers had unauthorized access to Marriott's cloud database for four years before detection, compromising 500 million records.

Mitigation Strategies :

- Enable Logging & Monitoring : Use AWS CloudTrail, Azure Monitor, Google Cloud Security Command Center.
- Use AI for Threat Detection : Implement AI-driven security analytic tools.

CONCLUSION:

To sum up, Cloud Computing is the term used to describe accessing the resources that are available at the remote locations like servers through millions of clients who are just browsing the content from remote servers. Cloud computing helps in maintaining programs and data on the internet rather than on your hard drive or computer. So, whenever you log into your Google Drive account or watch videos on YouTube, you are getting cloud computing benefits!

Christian, A. (2011). The Advantages of Using Cloud Computing. Retrieved from http://cloudcomputing.sys-con.com/node/1792026

REFERENCES

1. Haynie, M. “Enterprise Cloud Services: Deriving business value from cloud computing. Microfocus, Tech. Report, 2009.
2. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” 2008 10th IEEE International Conference on High Performance Computing and Communications, 200
3. Haynie, M. “Enterprise Cloud Services: Deriving business value from cloud computing. Microfocus, Tech. Report, 2009.
4. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” 2008 10th IEEE International Conference on High Performance Computing and Communications, 200
5. Haynie, M. “Enterprise Cloud Services: Deriving business value from cloud computing. Microfocus, Tech. Report, 2009.
6. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” 2008 10th IEEE International Conference on High Performance Computing and Communications, 200
7. Haynie, M. “Enterprise Cloud Services: Deriving business value from cloud computing. Microfocus, Tech. Report, 2009.
8. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” 2008 10th IEEE International Conference on High Performance Computing and Communications, 2008. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” 2008 10th IEEE International Conference on High Performance Computing and Communications, 2008
9. Marston, S, Li, Z, Bandyopadhyay, S, Zhang, J.and Ghalsasi, A, “Cloud computing—The business perspective”, Decision support systems,51(1),pp.176-189, 2011.
10. N. Taleb and E. A. Mohamed, “Cloud computing trends: A literature review,” Academic Journal of Interdisciplinary Studies, vol. 9, no. 1, p. 91,2020.
11. https://cloud.google.com/learn/what-is-cloud-computing/
12. https://www.geeksforgeeks.org/cloud-computing/security-issues-in-cloud-computing/
13. https://www.geeksforgeeks.org/cloud-computing/characristics-of-cloud-computing/

14. https://simple.wikipedia.org/Wiki/cloud_computing/
15. https://simple.wikipedia.org/wiki/Google_Custom_Search?action=edit&redlink=1
16. https://www.ibm.com/think/topics/rbac
17. https://www.fortra.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more
18. https://cloudsecurityalliance.org/blog/2024/10/09/top-threat-3-api-ocalypse-securing-the-insecure-interfaces
19. https://www.optiv.com/insights/discover/blog/insecure-api-cloud-computing-causes-and-solutions
20. https://www.getastra.com/blog/cloud/cloud-security-breaches/