Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

Security Issues And Challenges In Cloud Computing

[1]M.S. Ajitha Purnima, [2]Dr. Devendran, [3]Dr. Rajavarman

[1]Ph.D. Research Scholar, Dr. MGR Educational and Research Institute
[2]Associate Professor, Dr. MGR Educational and Research Institute
[3]Professor and Deputy Dean, Dr. MGR Educational and Research Institute

Abstract: Data is a very essential source for all organizations in today's world. In the past years data was stored in a sever which was physically placed inside the organizations. As the amount of data is been increasing, it is a great challenge for the Database Administrator to manage the database. The entire data was in the control of the Database Administrator. To overcome this challenge arose the concept of Cloud computing. It is a technique that describes software and services that run through the internet rather than private servers and hard drives. In cloud computing the consumers does not own the infrastructure needed to support the programs or any applications they use. The data is owned by a third party and the end users pay for the services provided to them. This paper discusses about the basics of cloud computing management and its types. Cloud provides various advantages to its users and at the same time the major concern is towards the security of data. The data is stored in the cloud and it can be accessed through internet only. Internet is playing a major role in everyone's life. The world has become too small and it is placed in the palm of a human. This is because of the technology that is ruling the world. To secure the data in cloud is a major and the most important task that should be looked into. This paper focusses mainly the security issues and challenges in cloud.
Keywords: Cloud Computing, Security Issues and Challenges, Community Cloud

1. Introduction

Cloud computing, delivers services like servers, storage, networking, software and more to its users over the Internet. Initially when computer was introduced, it was a major task to find space to place the system and maintain it. Gradually when the technology grew rapidly, everything became compact, the speed and reliability was increased. There were significant advancements in technology, leading to the modern computers we use today. One of the latest technologies we use in our modern world is Cloud computing. Cloud computing is a technology that allows users to access and store data, and run applications over the internet instead of on their local computers or servers.

Fig 1: Architecture of Cloud Computing

In essence, it enables the delivery of various services, including software, storage, and processing power, via the internet. Cloud computing providers maintain and manage the underlying infrastructure, ensuring users can focus on utilizing the services without worrying about hardware or software maintenance. This technology offers scalability, flexibility, and cost-efficiency, making it popular among businesses and individuals alike. It has various deployment models such as public, private, hybrid, and multi-cloud, catering to diverse user needs.

2. Types Of Cloud

There are four main types in cloud, they are:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

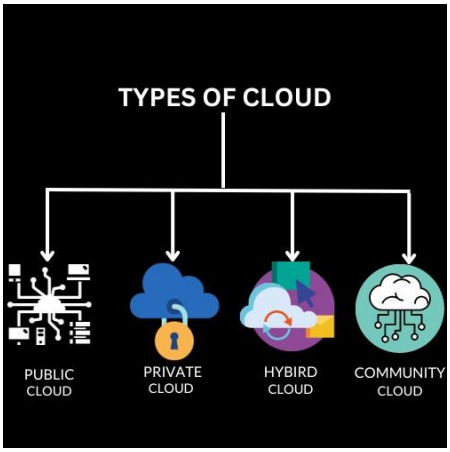

Fig 2: Types of Cloud

2.1 Private Cloud

In Cloud Computing, a private cloud refers to a computing environment that is exclusively used by a single organization. Unlike public clouds, which serve multiple organizations, a private cloud is dedicated to the needs and goals of a specific business or entity. A private cloud can be physically located on the organization's on-site data center or hosted by a third-party service provider. It can also be managed internally by the organization's IT team or by an external provider. The key feature of a private cloud is that it provides a secure and customizable cloud computing environment where the organization has complete control over its resources and infrastructure.

Private clouds are often chosen by businesses and government organizations that require a high level of control, security, and compliance due to regulatory or sensitive data concerns. Using a private cloud allows these organizations to leverage cloud computing benefits such as scalability and resource optimization while maintaining a higher degree of control over their data and applications. However, private clouds typically require higher upfront costs and ongoing maintenance compared to public cloud solutions.

2.2 Public Cloud

In cloud computing, the public cloud refers to a computing environment that is hosted by third-party service providers and made available to the general public or a large industry group over the internet. Public cloud services are typically offered on a pay-as-you-go model, where customers can access resources such as virtual machines, storage, and applications without owning or maintaining the underlying infrastructure.

Public cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), own and operate the infrastructure and offer services to multiple clients. These services can include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Public cloud solutions are scalable, flexible, and cost-effective, making them popular for businesses of all sizes to host websites, applications, and data without the need for significant upfront investments in hardware and software.

2.3 Hybrid Cloud

In cloud computing, a hybrid cloud refers to a computing environment that combines the use of both public and private clouds. This approach allows organizations to leverage the advantages of both cloud models while addressing specific business requirements and concerns.

In a hybrid cloud setup, some applications and data are hosted in a public cloud, while others are hosted in a private cloud infrastructure. These two cloud environments are integrated, allowing data and applications to

be shared between them. The connection between the public and private clouds is typically established through encrypted technology, ensuring secure data transfer and communication.

Organizations choose hybrid cloud solutions for various reasons, such as:

- **Scalability:** They can utilize the scalability of public clouds for handling variable workloads and peak demands while maintaining sensitive data in a private cloud.
- **Security and Compliance:** Sensitive data can be stored in the private cloud, ensuring higher levels of security and compliance with industry regulations, while less sensitive data or applications can be hosted in the public cloud.
- **Cost Efficiency:** Hybrid cloud allows organizations to optimize costs by using public cloud resources for non-sensitive workloads and private cloud resources for critical, sensitive applications, thereby balancing costs and performance.
- **Flexibility:** Businesses can move workloads between public and private clouds based on changing requirements, giving them the flexibility to adapt to evolving business needs.
- **Disaster Recovery:** Hybrid cloud setups can enhance disaster recovery capabilities. Critical applications and data can be mirrored in both public and private clouds, ensuring business continuity in case of failures.

Implementing a hybrid cloud strategy requires careful planning and integration to ensure seamless communication between the public and private cloud components while maintaining security and data integrity.

2.4 Community Cloud

In cloud computing, a community cloud refers to a shared computing environment that is tailored for specific communities or organizations with common concerns, goals, or compliance requirements. Unlike public clouds that are open to the general public or private clouds dedicated to a single organization, community clouds are shared by several related entities.

In a community cloud setup, multiple organizations from a specific industry, government sector, or research community share the cloud infrastructure and resources. These organizations collaborate to define the cloud's specifications, ensuring that it meets their collective needs, security standards, and compliance requirements.

Community clouds are beneficial for organizations facing similar challenges and regulatory constraints. By pooling resources and sharing costs, these organizations can achieve economies of scale while maintaining control over their data and applications. This shared infrastructure allows community members to securely collaborate, share information, and develop applications tailored to their specific industry requirements.

Community clouds are especially popular in sectors such as healthcare, finance, and government, where data security, privacy, and compliance with industry regulations are paramount. By utilizing a community cloud, organizations can benefit from the advantages of cloud computing while addressing their unique sector-specific needs.

3. Cloud Services

Cloud services refer to services delivered to users and organizations via the internet, utilizing the computing resources and infrastructure provided by cloud computing providers. These services can include a wide range of applications, storage, and processing power, and they offer several advantages such as scalability, flexibility, and cost-effectiveness. Here are some common types of cloud services

- **Infrastructure as a Service (IaaS):** IaaS provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and networking components on a pay-as-you-go basis. This allows businesses to avoid the cost and complexity of owning and maintaining physical servers and data centers.
- **Platform as a Service (PaaS):** PaaS provides a platform allowing customers to develop, run, and manage applications without dealing with the complexity of building and maintaining the underlying infrastructure. It typically includes development tools, database management systems, and application hosting, making it easier for developers to focus on creating software.

- **Software as a Service (SaaS):** SaaS delivers software applications over the internet on a subscription basis. Users can access these applications through a web browser, eliminating the need for installation and maintenance. Examples of SaaS include email services (like Gmail), office productivity suites (such as Microsoft 365), and customer relationship management (CRM) software like Salesforce.

Fig 3.1 Cloud Services

- **Function as a Service (FaaS)**: FaaS, also known as serverless computing, allows developers to run individual functions or pieces of code in response to specific events without managing servers. Cloud providers automatically scale the infrastructure as needed, and users are billed based on the actual usage of resources.
- **Storage as a Service:** This service provides scalable and secure cloud storage solutions. Users can store and retrieve data over the internet, and the storage capacity can be adjusted based on demand. Examples include Amazon S3 and Google Cloud Storage.
- **Database as a Service (DBaaS):** DBaaS offers database services hosted in the cloud. Users can access and manage databases without the complexities of hardware and software setup. Database providers handle maintenance tasks, ensuring data security and high availability.

Cloud services empower businesses and individuals to leverage advanced computing capabilities without the need for significant upfront investments in infrastructure. They are fundamental to modern IT architectures, enabling innovation, collaboration, and efficiency across various sectors.

4. Security Issues

Security is a paramount concern in the digital age, especially with the widespread use of cloud services and interconnected technologies. Several security issues are relevant in this context:

- **Data Breaches:** Unauthorized access to sensitive data can lead to data breaches, resulting in the exposure of personal information, financial data, or intellectual property. Proper encryption and access control measures are crucial to prevent such incidents.
- **Data Loss:** Data stored in the cloud can be lost due to various reasons, including accidental deletion, hardware failures, or cyberattacks. Regular backups and redundancy strategies are essential to mitigate data loss risks.
- **Identity Theft:** Cybercriminals can steal user credentials and impersonate individuals, gaining unauthorized access to accounts and sensitive information. Multi-factor authentication and strong password policies are vital to prevent identity theft.
- **Malware and Ransomware:** Malicious software can infect systems and networks, causing disruptions, stealing data, or encrypting files for ransom. Regular software updates, antivirus programs, and user education are key defenses against malware attacks.
- **Phishing Attacks:** Phishing involves tricking users into revealing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity. Security awareness training and email filtering systems help in detecting and preventing phishing attempts.

- **Insecure APIs:** Application Programming Interfaces (APIs) enable communication between different software applications. Insecure APIs can be exploited by attackers to gain unauthorized access. Regular security assessments and secure coding practices are essential for secure API usage.
- **Compliance and Legal Issues:** Organizations must adhere to various regulations and standards concerning data privacy and security. Failure to comply with these regulations can result in legal consequences and financial penalties.
- **Insider Threats:** Employees or individuals with insider access to systems and data can pose a significant security risk. Monitoring user activities and implementing strict access controls can help mitigate insider threats.
- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks overwhelm a target system with a flood of traffic, rendering it inaccessible to users. DDoS mitigation services and network security measures are essential to prevent such attacks.

Addressing these security issues requires a combination of technology, policies, and user awareness. Regular security audits, employee training, and staying updated with the latest security practices are vital to maintaining a secure digital environment.

To improve the security of data, an encryption and decryption methodology will be derived by comparing and analysing few algorithms like Blowfish encryption algorithm, International Data Encryption Algorithm (IDEA), Triple Data Encryption Standard (DES) algorithm, Rivest, Shamir, Adleman (RSA) algorithm, two fish algorithm and Advanced Encryption Standard (AES) algorithm.

5. Conclusion

This paper highlights the critical significance of security in cloud computing. As organizations increasingly migrate their operations to the cloud, ensuring robust security measures is paramount. Throughout this paper, we've explored various security challenges and solutions, emphasizing the need for encryption, multi-factor authentication, regular audits, and user awareness training. Cloud service providers and users must collaborate closely to establish a strong security posture, leveraging the latest technologies and best practices. By doing so, they can mitigate risks, safeguard sensitive data, and foster trust in cloud-based systems. As the landscape of cloud computing continues to evolve, ongoing research and vigilance are essential to adapt to emerging threats and ensure a secure digital environment for all stakeholders involved.

References

[1] Mell and T. Grance., The NIST definition of cloud computing, 2009. [Online]. Available: csrc.nist.gov/groups/SNS/cloudcomputing/ cloud-def-v15.doc

[2] Amazon Web Services, Amazon Elastic Compute Cloud (Amazon EC2), 2009, [Online]. Available: http://aws.amazon.com/ec2

[3] Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing V2.1., 2009, [Online]. Available: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[4] D.Booth, et. al. Web service architecture, 2004 [Online]. Available:http://www.w3.org/TR/ws-arch/

[5] M. Jensen. et. al. “On Technical Security Issues in Cloud Computing” IEEE International Conference in Cloud Conouting, pp.109-116, Sep 2009.

[6] M. Marlinspike, Null Prefix Attacks Against SSL/TLS Certificates, 2009

[7] M. McIntosh and P. Austel. “XML Signature Element Wrapping Attack and CounterMeasures” Workshop on Secure Web Service, pp.20-27, 2005.

[8] M. McIntosh and P. Austel. “XML Signature Element Wrapping Attack and CounterMeasures” Workshop on Secure Web Service, pp.20-27, 2005.

[9] N. Gruschka and L. L. Iacono. “Vulnerable Cloud: SOAP Meaage Security Validation Revisited” IEEE International Conference on Web Service, pp.635-631, Jul 2009.

[10] OASIS. Web services security: SOAP message security 1.1., 2004. [Online]. Available: http://www.oasisopen.

[11] org/committees/download.php/16790/wss-v1.1-spec-os- SOAPMessageSecurity.pdf
[12] US-CERT. (2004) Understanding Denial-of-Service Attacks. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-015.html