STM JOURNALS

Recent Trends in
Parallel Computing

https://journals.stmjournals.com/rtpc

ISSN: 2393-8749
Volume 11, Issue 1, 2024
January—April
DOI (Journal): 10.37591/RTPC

Review RTPC

Analysis of Security in Cloud Computing

B. Krishna[1,*], D. Madhan[1], U. Udayakumar[2], K. Sutha[2]

Abstract

These days, cloud computing is expanding quickly in the IT sector, offering a fresh approach to managing various information systems. The rapid pace of technological advancement highlights the importance of embracing and leveraging its advantages. Organizations transitioning to cloud-based information archiving demonstrate several key characteristics. These include enhanced IT infrastructure, the ability to manage remote access from any location in the world with a stable Internet connection, and the cost savings that come with using cloud computing. As we shift everything to a distributed environment and toward the concept of asset pooling and on-request management, security and privacy concerns are always paramount. This study provides an in-depth exploration of issues related to cloud security. The architecture, features, delivery strategy, and stakeholders of the cloud are all taken into consideration while looking into the security problem. This study examines some of the main security challenges related to implementing cloud-aware security solutions that might potentially safeguard the dynamic and constantly evolving cloud paradigm.

Keywords: Cloud computing, security, networking, databases, operating systems

INTRODUCTION

Cloud computing refers to a paradigm where computing resources, such as hardware and software, are provided over a network by external parties. Users access these resources remotely, often without needing to understand the underlying technology. This approach offers a centralized pool of configurable resources that can be accessed on-demand, like utility services like electricity or water [1].

Key features of cloud computing encompass self-service on-demand, extensive network accessibility, resource pooling, swift elasticity, and measured service as shown in Figure 1. It is a dynamic platform that provides virtualized resources transparently through the Internet [2].

The architecture of cloud computing is commonly divided into three layers: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These layers offer varying levels of control and customization to users. Cloud deployment models comprise public clouds (where the infrastructure is owned and managed by the service provider), community clouds (managed by a consortium of organizations), private clouds (managed by a single organization), and hybrid clouds (blending elements of the other models) [3].

Cloud computing represents a revolutionary shift in how technology resources are utilized, offering a model where computational power and applications are accessed through the internet, hosted by third-party providers. This model enables users to leverage a vast array of services without the complexities of managing physical hardware and software resources.

***Author for Correspondence**
B. Krishna
E-mail: bk2229@srmist.edu.in

[1]Student, Department of Computer Science & Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India

Received Date: February 16, 2024
Accepted Date: March 08, 2024
Published Date: April 04, 2024

Citation: B. Krishna, D. Madhan, U. Udayakumar, K. Sutha. Analysis of security in cloud computing. Recent Trends in Parallel Computing. 2024; 11(1): 35–40p.

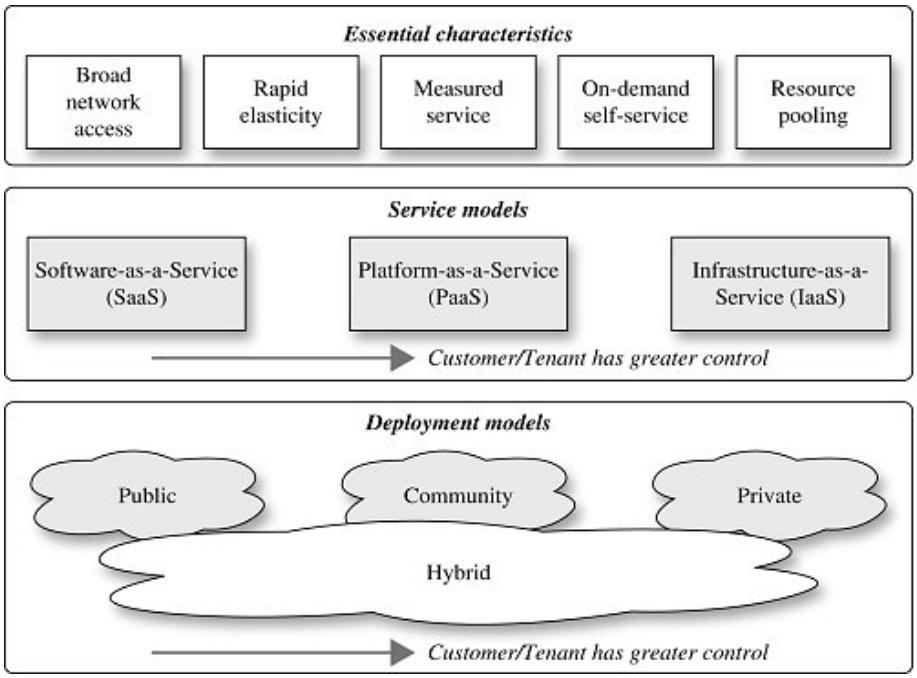

Figure 1. Cloud deployment model: an overview.

Central to its appeal is the abstraction of technology infrastructure, allowing users to benefit from cutting-edge computing capabilities [4].

Key to cloud computing's value proposition are its five foundational characteristics: on-demand self-service, where users can provision resources without human intervention; broad network access, ensuring services are available over the network and accessible through standard mechanisms; resource pooling, which combines computing resources to serve multiple consumers; rapid elasticity, allowing services to be scaled in accordance with demand; and measured. The service aims to offer transparency for both the provider and consumer of the service being utilized [5].

Deployment models of cloud computing vary based on the specific needs and policies of users, including public clouds, managed by external organizations offering services to the general public; community clouds, shared by several organizations with common concerns; private clouds, operated exclusively for a single organization; and hybrid clouds, which blend public and private cloud models to balance the need for scalability with the need for control over sensitive data [6].

Cloud Computing Applications

There are many daily life applications for cloud computing which we may not notice; it has made many online or internet service very efficient and affordable or even made it free of cost; we have applications like YouTube, Netflix and Social media platforms like Instagram, which use cloud storages to store the enormous data that they possess and stream it to the public for free or pay per use. Cloud storage also has other applications like File hosting services, Secure storage for personal data, Backup storage for Systems sites and software and Bigdata analysis. These services can be accessed through web with just stable and secure internet connection. Cloud computing has made our life simpler and made resource availability cost effective and simpler [7].

KEY SECURITY ISSUES IN CLOUD COMPUTING

Like mentioned above Cloud computing provides many services like PaaS, SaaS, and IaaS. Cloud computing integrates a variety of segments, each delivering distinct services and products to both individuals and organizations globally. This intricate system involves a variety of technologies,

including networking, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control, and memory management. Given this complexity, the security challenges inherent to these individual components also extend to cloud computing as a whole [8].

Identifying and addressing the primary security concerns within cloud computing is crucial. Below are some key security areas that require vigilant management:

1. *Data Security and Privacy:* Guaranteeing the confidentiality, integrity, and accessibility of data is of utmost importance. This involves safeguarding data against unauthorized access and ensuring the preservation of data privacy.
2. *Identity and Access Management (IAM):* Effective IAM ensures that only authorized users can access specific resources. This involves managing identities, authentication mechanisms, and access controls [9].
3. *Infrastructure Security:* Protecting the underlying infrastructure, including the physical and virtual resources, is critical to safeguarding the services running on them.
4. *Network Security:* Safeguarding the network entails implementing measures to protect data during transit. This encompasses encryption, secure communication protocols, and systems for detecting and preventing intrusions.
5. *Compliance and Legal Issues:* Adhering to regulatory and legal requirements is necessary to avoid penalties and ensure that cloud services are used ethically and legally [10].

By focusing on these areas, organizations can adopt cloud computing solutions with confidence, knowing that they are taking proactive steps to mitigate security risks.

- Data location,
- Data transmission,
- Virtual Machine security,
- Network security, and
- Access control.

Data Location

Selecting the optimal data center location to host your virtual infrastructure and data is pivotal in mitigating the risks and costs associated with unexpected downtime. Conversely, an ill-suited data center location can result in significant challenges. Here are four key considerations to bear in mind when assessing a cloud service provider's data center and their geographical placement:

1. *Proximity to Users:* Select a data center location that is near your users. This choice can minimize latency and enhance the overall performance of your applications and services.
2. *Regulatory Compliance:* Verify that the chosen data center location adheres to applicable regulations and standards. This is particularly vital for industries with stringent data protection requirements, such as healthcare and finance.
3. *Natural Disaster Risk:* Evaluate the likelihood of natural disasters in the selected data center location, such as earthquakes, floods, or hurricanes. Selecting a location with a low risk of such events can help minimize downtime and data loss.
4. *Security and Physical Infrastructure:* Evaluate the security measures and physical infrastructure of the data center. Look for features such as 24/7 security monitoring, access controls, and redundant power and cooling systems to ensure the safety and availability of your data.

By considering these factors, you can make an informed decision when selecting a data center location for your cloud infrastructure, helping to minimize downtime and maximize the reliability of your services.

- Latency,
- Location,
- Compliance, and
- Connectivity.

Latency plays a crucial role in influencing the performance of applications and the speed at which data is accessed. Low latency is essential for optimal application performance, while high latency can lead to frustration and delays. Geographical distance is a key factor impacting latency, and increased distances lead to elevated latency. To minimize latency, many companies choose to keep their production data on premises, close to their main office, to ensure that data travels a short distance, typically no more than a few miles.

When considering data center best practices, it is recommended to maintain a copy of your data at least 500 miles away from your primary location to ensure geographic redundancy. This distance helps mitigate the risk of regional disasters while keeping latency within acceptable limits. By balancing these factors, organizations can ensure both data resilience and optimal performance.

Compliance: There are specific globally acknowledged data compliance standards outlined below that departments can adhere to during the adoption of a cloud platform.

- ISO 27K Family standards;
- PCI-DSS Standards; and
- SSAE 16/ SOC 2.

These are several of the international standards that data centers or data warehouses should adhere to when managing client data.

Connectivity: We need lightning-fast connectivity in the Data Centre which ensures that data can be transmitted, accessed, and processed effectively, supporting a range of business operations and services.

Data Transmission

Network classifications span various types, including shared vs. non-shared, public versus private, and networks spanning from small to large geographical areas. Each category faces its unique set of security challenges. Network security issues include DNS attacks, where users might be redirected to malicious servers despite using domain names due to IP address feasibility challenges. Although DNS security measures like DNSSEC can mitigate threats, rerouting through malicious connections remains a concern. Sniffer attacks capture unencrypted data packets, risking the exposure of vital information across the network. Detecting sniffers can be done using ARP and RTT-based platforms. The reuse of IP address poses a security risk when the old address is assigned to a new user before being cleared from DNS caches, potentially compromising the privacy of the original user. Secure data transmission is crucial to prevent interception during communication between your site and the cloud provider or between services.

Securing data during transmission involves several key steps: encrypting the data prior to sending it, verifying the identities of the sending and receiving parties, and upon receipt, decrypting the data and confirming its integrity. For instance, Transport Layer Security (TLS) is commonly employed to safeguard data as it moves across networks, while Secure/Multipurpose Internet Mail Extensions (S/MIME) is frequently utilized to encrypt email communications.

VM Security

Virtualization stands as a cornerstone of cloud computing, driving its key advantages. Yet, it introduces certain security vulnerabilities, particularly concerning data protection. One significant risk involves the potential compromise of the hypervisor. This critical component, if found vulnerable, could jeopardize the entire system and the data therein.

Hypervisors, serving as the linchpin for virtual machines (VMs) on a platform, attract attention as prime targets for cyber-attacks. A breach in the hypervisor's security could lead to system-wide compromises. Additionally, the coexistence of multiple VMs on a single infrastructure amplifies the

security challenges. In these environments, side-channel attacks, which exploit information obtained from the physical implementation of a computer system rather than vulnerabilities in the code, present a distinct threat. Furthermore, malicious code embedded within a VM image can proliferate as the VM is cloned, intensifying the security risks.

Addressing these concerns necessitates a strategic approach to virtualization use. This includes judicious resource management and rigorous authentication processes before resource reallocation.

Network Security

Various encryption techniques can be employed to safeguard data during transit. Like Block ciphers encrypt data by applying a cryptographic key and algorithm to fixed-size blocks, preventing identical blocks from being encrypted the same way. Usually, the encryption of the next block is influenced by the ciphertext of the preceding block. Stream ciphers, on the other hand, encrypt each bit individually, depending on the current state of the cipher, creating a stream of encrypted bits. These methods play a crucial role in cloud data security, with their application varying based on specific scenarios and emphasizing the importance of securing data in both private and public clouds.

Stream ciphers, also known as state ciphers, encrypt data based on the current state of the cipher. Unlike block ciphers, they operate on each individual bit of the data. Using an encryption key and algorithm, each bit is processed one at a time. Stream ciphers, also known as state ciphers, encrypt data based on the current state of the cipher. In a stream cipher, each bit of data is encrypted individually using an encryption key, producing a stream of encrypted bits. Using a decryption key, the stream can be deciphered to recover the original plaintext.

Access Control

Access control stands as a pivotal framework in the realm of information security, significantly reducing the risk of unauthorized access to sensitive information. It employs a multifaceted approach to ensure data protection. Initially, it authenticates the identity of individuals attempting to access specific resources. Following this, it evaluates their authorization to access the resource and finally determines the extent of their permissions, which may include reading, editing, or deleting the resource.

CONCLUSION

In concluding the analysis of security in cloud computing, it is evident that while cloud computing offers significant benefits in terms of scalability, efficiency, and cost-effectiveness, it also introduces complex security challenges.

Technologies such as encryption, identity and access management, and intrusion detection systems play a critical role in securing cloud environments. A comprehensive security strategy that includes regular security assessments, adherence to best practices, and a culture of security awareness is essential for mitigating risks. Additionally, collaboration between cloud service providers and clients is crucial to ensure that security measures align with specific organizational needs and regulatory requirements.

As cloud computing undergoes further development, the security threats it encounters will also evolve. Therefore, ongoing research, development, and adaptation of security measures are imperative to safeguard the ever-expanding cloud ecosystem. Ultimately, the goal is to achieve a balance between leveraging the benefits of cloud computing and minimizing the potential security risks to ensure a secure and trustworthy cloud environment for all users.

REFERENCES

1. Mell P, Grance T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, US Department of Commerce. Special Publication 800–145. 2011. DOI: 10.6028/NIST.SP.800–145.

2. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl. 2011; 34(1): 1–11. DOI: 10.1016/j.jnca.2010.07.006.
3. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. J Internet Serv Appl. 2013; 4(1): 5. DOI: 10.1186/1869–0238–4–5.
4. Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in Cloud. J Netw Comput Appl. 2013; 36(1): 42–57. DOI: 10.1016/j.jnca.2012.05.003.
5. Aljawarneh S, Aldwairi M, Yassein MB. Cloud security: Challenges and future trends. Cybersecurity. 2018; 1(1): 9. DOI: 10.1186/s42400–018–0010–6.
6. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst. 2012; 28(3): 583–592. DOI: 10.1016/j.future.2010.12.006.
7. Rittinghouse JW, Ransome JF. Cloud Computing: Implementation, Management, and Security. CRC Press; Florida, United States. 2016. ISBN: 978–1–4398–0680–7.
8. Takabi H, Joshi JBD, Ahn GJ. Security and Privacy Challenges in Cloud Computing Environments. IEEE Secur Priv. 2010; 8(6): 24–31. DOI: 10.1109/MSP.2010.186.
9. El-Zoghby AM, Azer MA. Cloud computing privacy issues, challenges and solutions. 2017, IEEE 12th International Conference on Computer Engineering and Systems (ICCES). 2017 Dec; 154–160. DOI:10.1109/ICCES.2017.8275295.
10. Hassan J, Shehzad D, Habib U, Aftab MU, Ahmad M, Kuleev R, Mazzara M. The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR). Computer Intel Neurosci. 2022 Jun 7; 2022: 8303504. Published online 2022 Jun 7. Doi: 10.1155/2022/8303504. PMCID: PMC9197654, PMID: 35712069.

