International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 579-582, October-2023
https://doi.org/10.47001/IRJIET/2023.710076

Cloud Computing Security

[1]Prof. S.K.Totade, [2]Priyanka Bhumbar, [3]Vaishnavi Samudre, [4]Lalita Darsimbe

[1]Assistant Professor, Department of MCA, Vidya Bharati Mahavidyalaya, Amaravati, India
[2,3,4]Student, Department of MCA, Vidya Bharati Mahavidyalaya, Amaravati, India

Abstract - Cloud computing refers to the management of data and servers and the provision of technology services using cloud computing technology. It is commonly used to store large amounts of data on cloud platforms. As a result, it is essential to safeguard data in various formats such as text, audio, video, and others. This paper presents a research study on cloud security, focusing on AWS, the most trusted cloud computing provider. AWS offers not only cloud security but also cloud storage services. The document addresses several key security challenges, including virtualization security, data storage in the cloud, and risk tolerance assessment in cloud computing. As the cloud grows, it is increasingly important to understand and implement effective security measures to protect sensitive information and maintain trust in cloud-based services.

Keywords: Cyber Security, Virtualization, Scalability, Cloud Service provider, Storage security, Data integrity and Data confidentiality.

1. Introduction

Cloud computing refers to the practice of storing and accessing data and programs on remote servers hosted on the internet, rather than on a computer's hard drive or local server. The term "cloud" simply means the servers that are accessed over the internet. Cloud providers usually offer a "pay-as-you-go" model, which may result in unexpected operating expenses if administrators are not familiar with cloud pricing models. Essentially, cloud computing allows users to access data and applications from anywhere, at any time, as long as they have an internet connection. This technology has become increasingly popular due to its flexibility, scalability, and cost-effectiveness.

Service providers:

- Google Cloud
- AWS(Amazon web server)
- Microsoft Azur
- IBM Cloud
- Alibaba Cloud

Cloud providers offer types of services:

1) Infrastructure as a Service (IaaS): Which provides hardware-related services through cloud computing.

2) Platform as a Service (PaaS): Which provides a cloud development platform. However, different vendors offer incompatible platforms.

3) Software as a Service (SaaS): Which offers complete software services in the cloud.

Cloud computing security concerns include sensitive data access, sharing, privacy, authentication, hacking, recovery, accountability, and account control.

2. Security Analysis

ECC encryption efficiently encrypts messages by utilizing varying points on an elliptic curve. This method uses a short key size of 256 bits which makes it difficult for algorithms to attack the encryption system as the computing complexity of attacking algorithms is O (2^128). Cloud clients' IDs and private keys are stored in their smart cards to prevent illegal users from generating a valid digital signature.

3. Security Architecture

When designing cloud security architecture, it is crucial to define the objectives. The architecture must address three key factors: the attack surface that represents external access interfaces, the protected asset set that contains the information being safeguarded, and vectors intended to perform indirect attacks, including those in the cloud and attacks on the system.

To achieve the goal of cloud security architecture, a set of functional elements must be implemented. These elements are often treated as separate entities rather than being part of a coordinated architectural plan. They include access control, network security, application security, contractual security, and monitoring, also called service security. Additionally, data protection measures are implemented at the protected asset level.

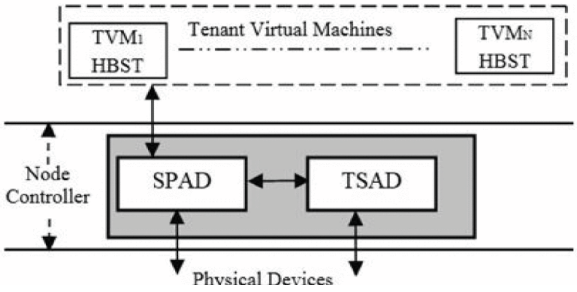
A comprehensive cloud security architecture brings together the functional elements to achieve the objectives.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 579-582, October-2023

https://doi.org/10.47001/IRJIET/2023.710076



4. Security

Cloud security is crucial to protecting data that is either stored or moving in and out of the cloud. It is designed to protect your data from various security threats like unauthorized access, theft, and corruption. The concept of cloud security relies on physical security, technology tools, access management and controls, and organizational policies. These pillars form the basis of any organization's security program.

The three key concepts of cloud security are as follows:

- **Data confidentiality:** It ensures that data can only be accessed or modified by authorized people or processes. The organization must take measures to keep its data private.
- **Data integrity:** This concept ensures that data is trustworthy, accurate, authentic, and reliable. To maintain data integrity, organizations must implement policies or measures that prevent the data from being tampered with or deleted.
- **Data availability:** While unauthorized access must be stopped, data must still be available and accessible to authorized people and processes when required. Therefore, the organization must ensure continuous uptime and keep systems, networks, and devices running smoothly to ensure data availability.

5. Security Issues In Cloud Computing

Data Loss

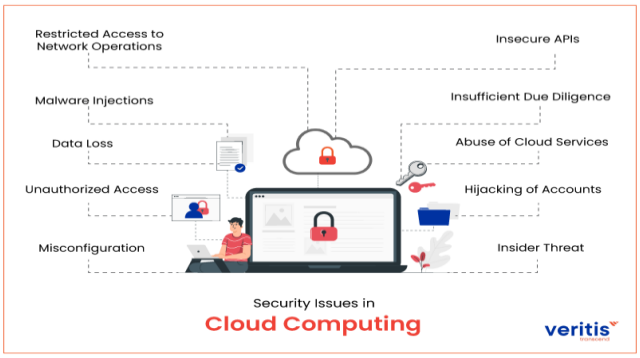
Cloud computing faces a significant challenge - data loss, commonly referred to as a data leak. Insiders, such as employees and business partners, who have access to sensitive data, can enable hackers to compromise the security of a cloud service and gain access to private and confidential information.

Malware injection

Malware injections are scripts or code fragments inserted into cloud services, operating as Software as a Service from cloud servers, and mimicking "genuine instances". This implies that malicious code can infiltrate cloud services and appear to be part of the program or service running on cloud servers themselves.

Insider Threat

Insider threats in companies are a real possibility, even though they may seem unlikely. Authorized employees who have access to a company's cloud-based services can exploit or obtain sensitive data such as client accounts, financial forms, and other vital information. Furthermore, insiders do not necessarily have to be malicious to pose a threat.



6. Cloud Security Solution

Cloud Workload Protection Platforms are tools used to reduce security risks by identifying vulnerabilities in static code, performing system hardening, and detecting workload misconfigurations. These agent-based tools use a variety of tactics such as network segmentation and system integrity protection to provide security at a workload level.

It is important to note that CWPPs do not provide coverage at the data or application layer. Furthermore, they exclude runtime security when it comes to defending containers, which is a critical component of advanced threat detection and response.

7. Network Detection And Response

Network Detection and Response tools are a security approach that uses network data to defend against cloud threats and to secure containers. These tools are very effective in detecting post-compromise behaviors within the perimeter and are an essential component of defense-in-depth strategies. Since all workloads communicate through the network, network data is important for security analysts, incident responders, and forensic investigators.

While on-premises security has been using network-based tools for years, collecting network data in cloud environments has been challenging in the past. However, with network taps from major cloud service providers and third-

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 579-582, October-2023

https://doi.org/10.47001/IRJIET/2023.710076

party packet brokers, much of the complexity and friction that came with NDR in the cloud has been eliminated.

8. Cloud Access Security Brokers

Breaches can happen due to misconfigured cloud settings, weak access controls, or insider threats. When confidential data is stored in the cloud, it becomes vulnerable to cybercriminals. Therefore, it is of utmost importance to ensure that only authorized individuals have access by managing user identities, permissions, and access controls across a dynamic cloud environment. Proper management of these controls is essential to mitigate the risk of unauthorized access and data breaches.

When it comes to securing applications, Static Application Security Testing (SAST) is an essential measure. While encrypting data in transit and at rest is crucial, managing encryption keys can become challenging, especially in multi-cloud or hybrid environments. Misconfigurations in cloud services can create vulnerabilities, making it critical to configure security measures properly.

Cloud resources often lack visibility into their security posture, but CSPM tools can help in complex environments.

Cloud Infrastructure Entitlement Management

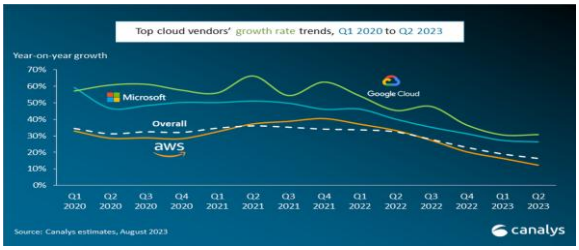
It is crucial to implement DDoS protection measures. Developing and testing an effective incident response plan specific to cloud environments is also important.

9. Cloud Security Challenges

Data breaches can occur due to misconfigured cloud settings, weak access controls, or insider threats. When sensitive information is stored in the cloud, it becomes a target for cybercriminals. Therefore, it is crucial to ensure that authorized individuals have access by managing user identities, permissions, and access controls across a dynamic cloud environment. It is important to understand the shared responsibility model, where the cloud provider secures the infrastructure, but users are responsible for securing their data and applications. Encrypting data both in transit and at rest is essential, but key management can be challenging, especially in multi-cloud or hybrid environments. Misconfigurations in cloud services can cause vulnerabilities, making it critical to configure security groups, firewalls, and access controls correctly. Maintaining visibility into the security of cloud resources can be challenging without the right tools, especially in large and complex cloud environments. Cloud services are also prone to Distributed Denial of Service (DDoS) attacks, which can disrupt operations. Therefore, it is crucial to implement DDoS protection measures. Finally, developing and testing an effective incident response plan specific to cloud environments is crucial to minimize the impact of security incidents.

10. Cloud Vendor's Growth

Global spending on cloud infrastructure services increased by 16% to reach $72 billion in the second quarter of 2023. Although this growth rate represents a slowdown from the previous quarter's 19%, it can be attributed to market pressures. Additionally, slower growth is also due to the market's larger size.



In the same quarter, AWS, Microsoft Azure, and Google Cloud, the top three vendors, collectively grew by 20%, accounting for 65% of total spending. While AWS and Microsoft both experienced a deceleration in growth, Google Cloud's growth rate remained steady from the previous quarter at 31%.

11. Conclusion

Cloud security is a sophisticated technology that provides computing and access to high-performance computing, storage, and infrastructure through the Internet. Cloud computing has significantly impacted the computer industry, including software companies and internet service providers. It is an ever-growing part of the IT industry and is provided by cloud service providers (CSPs). The key technology used to develop cloud security is virtualization.

In the future, work on data science, artificial intelligence, and machine learning services should be prioritized inside cloud providers to protect customer-sensitive data such as login credentials through encryption techniques and other password protection techniques inside the security group. This will increase efficiency and accuracy and make the data more secure. Multi-factor authentication should be practiced to protect the data. Frequent clearing of cache and cookies is recommended, and passwords should never be auto-saved in the browser.

REFERENCES

[1] https://www.javatpoint.com/what-is-cloud-security

[2] https://www.geeksforgeeks.org/cloud-computing-security/

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 579-582, October-2023
https://doi.org/10.47001/IRJIET/2023.710076

[3] https://www.geeksforgeeks.org/security-issues-in-cloud-computing/amp/#amp_tf=From%20%251%24s&aoh=16972181138706&referrer=https%3A%2F%2Fwww.google.com

[4] https://www.tutorialrsweb.com/cloud-computing/cloud-computing-11.htm

[5] https://www.educba.com/

Citation of this Article:

Prof. S.K.Totade, Priyanka Bhumbar, Vaishnavi Samudre, Lalita Darsimbe, "Cloud Computing Security" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 10, pp 579-582, October 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.710076

****

