WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on Cloud Computing Security Issue

Bhavana PG[1], Dr. Bhuvana J[2]

[1]Student of MCA, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India
[2]Assistant Professor, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India
Doi: https://doi.org/10.55248/gengpi.5.0324.0809

ABSTRACT:

Cloud computing represents a modern computing paradigm, offering a collection of accessible resources and services over the internet or a network. It provides an abstraction layer that facilitates convenient, on- demand access to a shared pool of configurable computing resources, such as servers, storage, and networks, which can be rapidly provisioned and released with minimal management overhead. The adoption of cloud computing has been widespread across various industries, including banking, healthcare, retail, education, manufacturing, and business, primarily due to the efficiency of pay-per-use models that grant access to networks, storage, servers, services, and applications without the need for physical ownership. However, the lack of direct control over data poses significant security challenges in cloud computing, including risks of data loss, unauthorized access, and traffic interception. This study aims to delve into several aspects of cloud security, including availability, elasticity, and multi-tenancy. Furthermore, it explores current security methodologies and strategies aimed at ensuring a secure cloud environment. By examining various security threats, models, and tools, both researchers and industry experts can gain insights into safeguarding cloud infrastructures effectively while addressing emerging security concerns.

KEYWORDS: Security issues, Cloud Security, Cloud Architecture, Challenges of IT industry.

Introduction

cloud computing has emerged as a transformative force within the IT industry, profoundly impacting data storage, security, accessibility, and cost-efficiency. With the proliferation of the internet and the escalating costs associated with hardware and software, the concept of cloud computing has gained immense traction. It offers a paradigm where services are delivered online upon user request, aiming to mitigate the expenses of hardware and software procurement. Despite its rapid adoption and myriad benefits, cloud computing confronts several challenges related to data storage and secure access. Issues such as vendor lock-in, multi-tenancy, loss of control, service disruption, and data loss underscore the critical importance of cloud security within the realm of cloud computing research and practice. As the field continues to evolve, addressing these challenges remains paramount to harnessing the full potential of cloud computing while ensuring the integrity, confidentiality, and availability of data and services.

I. Architecture

SAAS Software As A Service: Pay per usage of software rather than owning it.
PAAS Platform As A Service: Outsider supplier appropriates equipment.
IAAS Infrastructure As A Service: entails providing computing infrastructure in the form of on-demand services

A. *Software as a service:*

It enables customers to pay for software based on their usage over time, with pricing influenced by market demand and supply dynamics. SaaS, also known as cloud application services, operates on a web-based delivery model managed by third-party vendors, allowing users to access applications through an interface. One of the key features of SaaS is its scalability and flexibility. Users can easily scale up or down their usage of software based on

their needs, without the need for significant infrastructure investments or IT overhead. This scalability is particularly beneficial for businesses with fluctuating demand or growth patterns. Another advantage of SaaS is its accessibility. Users can access SaaS applications from any internet-enabled device, providing flexibility and convenience for remote work, collaboration, and mobile productivity. While some SaaS applications may require plugins, many can be accessed directly from a web browser without the need for downloads or installations. Vendors handle various tasks including servers, virtualization, runtime, data management, middleware, operating systems, and networking, ensuring the reliability and support of SaaS initiatives.

Examples of SaaS providers include Cisco, AWS, and Google Cloud.

Advantage of SAAS:

- Reduced time to benefit.
- Scalability
- Elasticity
- Security

B. *Platform as a service*

Platform as a Service (PaaS) is utilized to furnish cloud components for software and other projects, commonly referred to as cloud platform services. PaaS facilitates the acceleration, simplification, testing, and cost reduction of application development and deployment processes. PaaS encompasses a range of components essential for supporting the web application life cycle, including servers, storage, networking, middleware, database management systems, development tools, and business intelligence. PaaS providers offer a variety of resources such as programming languages, application frameworks, databases, and additional tools to streamline development and deployment activities. In essence, PaaS furnishes a robust and adaptable platform for developing, deploying, and scaling applications in the cloud. By abstracting infrastructure complexities, PaaS empowers developers to innovate swiftly and deliver top-notch software solutions that meet the evolving needs of businesses and users.

Advantages of PAAS:

- Scalability
- Elasticity
- Security
- Pay as you go

C. *Infrastructure as a service:*

Infrastructure as a Service (IaaS) represents a fundamental layer within the cloud computing platform, enabling customers to delegate their IT infrastructures, including servers, networking, processing, storage, virtual machines, and various resources. The advent of the IaaS cloud computing layer eliminates the necessity for firms to maintain their IT infrastructure. Currently, a multitude of IaaS providers offer databases, message queues, and other services above the virtualization layers. Unlike Software as a Service (SaaS) and Platform as a Service (PaaS), where clients relinquish control over runtime, middleware, applications, data, and operating systems, IaaS clients retain responsibility for these aspects. This distinction underscores the level of autonomy and control that IaaS clients maintain over their infrastructure and operating environments within the cloud computing landscape.

Advantages of IAAS:

- Scalability
- Elasticity
- Security
- Pay as you go

II. Cloud Security Issues

Companies utilizing cloud platforms must prioritize enhanced security while enabling remote access for team members, clients, and stakeholders to reach their online data and applications. It is crucial for businesses to recognize the security threats linked with cloud computing, given the annual growth in cloud storage and application usage.

Organizations adopt various cloud models, including public, private, and hybrid, and leverage a range of cloud services like IaaS, PaaS, and SaaS. These models and services are susceptible to numerous cloud security vulnerabilities. There are certain problems with every service model. First, there are two perspectives on security issues. The first is

from the service provider, who guarantees the security of the services they offer and oversees the identity management of their clients. Another perspective is that of the consumer, who verifies that the service they are utilizing is sufficiently secure.

A. *Security System Misconfigurations:*

A 2021 study conducted by Trend Micro, analyzing data from Amazon Web Services (AWS) and Microsoft Azure cloud platforms, revealed that approximately 65–70% of all cloud security vulnerabilities stem from security system misconfigurations. Several factors contribute to these misconfigurations:

- One significant challenge arises from the inherent design of cloud architecture, which prioritizes accessibility and data sharing, making it difficult for cybersecurity experts to ensure that only authorized parties can access data.
- Additionally, organizations leveraging cloud services must depend on the security configurations established by their chosen cloud service provider (CSP), relinquishing some level of insight and control over their infrastructure. This reliance on CSPs underscores the importance of selecting a reputable and dependable CSP for ensuring robust security measures.

B. *Loss Resulting from Cyberattacks:*

For cybersecurity experts, protecting an entirely or partially migrated network from all kinds of intrusions presents special difficulties. Due to their widespread accessibility over the public internet, cloud-based networks are frequently the target of cybercriminals. A successful hack on one target can be replicated by attackers to get access to numerous others, as different Data firms frequently share the same CSP.

C. *Unsecure Access Control Points:*

The ability of cloud networks to be accessed from any location, enabling connections between teams and consumers regardless of location, is one of their primary draws. However, inadequate configuration and optimization of cloud security often leave critical technologies, such as application programming interfaces (APIs), vulnerable to attacks. Implementing online application firewalls is crucial to verify the authenticity of all HTTP requests, thus preventing hackers from exploiting these vulnerabilities as entry points. By doing so, organizations can ensure the continuous protection of online applications and processes reliant on APIs.

D. *Inadequate Threat Notifications and Alerts*:

The speed at which website or security staff can receive threat notices and alerts is a fundamental component of any successful network or computer security solution. The same applies to cloud-based solutions. Instant notifications and alarms enable proactive threat mitigation, effectively preventing successful hacks and minimizing potential damages.

E. *Elasticity:*

Elasticity can be characterized as a system's ability to adjust to changes in workload by autonomously allocating and distributing resources so that, at any one time, the available resources roughly match the demand that is currently present. Scalability follows from elasticity. Customers are said to be able to scale up or down based on necessity. Tenants that were previously assigned a resource can now use it thanks to this scalability. Confidentiality problems could arise from this, though.

F. *Insider attacks:*

cloud model adopts a multitenant approach, consolidating under a single management domain for the provider, presenting an internal threat that organizations must contend with. Hiring guidelines and providers do not exist for cloud workers. Thus, it is simple for a third-party vendor to hack into an organization's data, corrupt it, or sell it to another business.

G. *Outsider attacks:*

This is a serious worry for organizations as it exposes confidential information. Clouds differ from private networks due to their increased number of interfaces. Hackers and attackers may exploit API vulnerabilities to disrupt connections.

H. *Network Security:*

- Denial Of Service attack: An occurrence like a machine or network crashing can render it inaccessible to users. Malicious attackers have the ability to either provide specific information to the target, leading to its shutdown, or inundate it with traffic, resulting in a crash.
- Man in the middle attack: The attacker initiates an autonomous connection and interacts with the cloud user via its separate network, ultimately obtaining full control.
- Port scanning: A port is a site where the data is internally exchanged. When subscribers configure a group, port scanning occurs. Configuring the internet automatically scans ports, which can pose security risks.

I. *Account Hijacking*:

One of the main issues in society is hijacking. There can be multiple reasons regarding this such as Sharing credentials and data with third-party vendors for online transactions, among other things. Attackers that steal our account may edit data, change transaction details, and utilize other cloud services to carry out further attacks.

J. *Cloud service abuses*:

Cloud abuse remains a significant threat, particularly when hackers exploit social media platforms to pilfer codes and disrupt the cloud environment. Organizations may encounter challenges like system shutdowns and data loss as a result. To mitigate this concern, it's crucial to identify assets, analyze critical information, recognize threats and vulnerabilities, evaluate risks, and implement protective measures and security layers.

III. TECHNIQUES TO SECURE DATA IN CLOUD:

A. *Identity management and Authentication:*

Cloud identity encompasses a collection of technologies, protocols, and practices designed to manage and regulate user identities and access to digital resources within cloud-based environments. Its major purpose is to provide secure authentication, authorization, and administration of user access across several cloud services and applications.

- Authentication as a service: Authentication as a Service (AaaS) offers a cloud-based approach to user authentication. Online services have the capability to seamlessly integrate AaaS into their applications, guaranteeing robust and secure user authentication across distributed services. Organizations gain from a consistent authentication process, reducing the necessity for numerous application-specific implementations.
- Identity as a service: IDaaS provides a service for identity management. Users have a steady identity and similar experience across multiple applications, while application developers save the overhead of creating and operating identity management internally.

Cloud identity providers offer essential services, including:

- Single Sign-On (SSO): Single Sign-On (SSO) simplifies the authentication process by enabling users to log in once and access multiple accounts without the need for repetitive authentication.
- Multi-Factor Authentication (MFAMFA implements security by requiring users to present multiple methods (e.g., password, biometrics, trusted device) during authentication.
- Identity Management: This involves tracking user identities, verifying their identity, provisioning access, and managing authentication throughout the account lifecycle.

B. *Data Encryption:*

When storing sensitive information in a large data repository, it's crucial to implement encryption methods. While passwords and firewalls offer some level of protection, they can still be circumvented for unauthorized access to data. Encrypted data remains unreadable without the corresponding key, rendering it useless to any unauthorized individuals. Encryption involves converting data into a confidential code, requiring the encryption key or password to decipher the encrypted data.

C. *Privacy and Information integrity:*

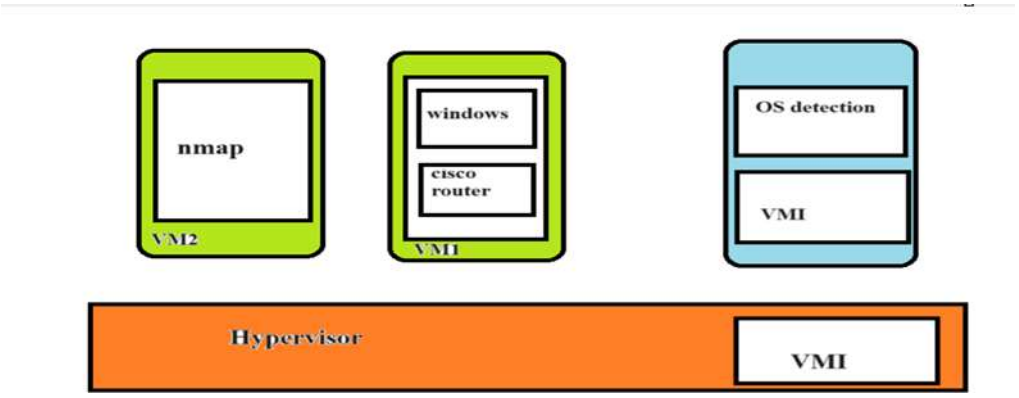
In cloud computing, legitimate users access information and resources, which are available through web browsers but can also be targeted by malicious attackers. Establishing mutual trust between providers and users is an effective means of maintaining information integrity. Authentication, permission, and accounting controls can be deployed across various levels to ensure authorized usage of resources. Secure access methods, such as RSA certificates and SSH-based tunnels, can be employed to enhance security.

D. *Availability of information (SLA):*

The absence of data or information availability poses a significant concern within cloud computing services. Service Level Agreements (SLAs) serve to inform users about the accessibility of network resources, fostering a trusting relationship between customers and providers. Implementing backup plans for both local resources and critical information ensures resource availability, enabling users to access information even in the event of unavailability.

E. *Securing the information:*

This information security strategy entails gathering data into a centralized repository. It comprises agents installed on the systems to be monitored, which then transmit information to a server referred to as the "Security Console." The Security Console is managed by an administrator who reviews the information and addresses any alerts. As the cloud user base and dependency stack expand, the cloud security processes employed to address security concerns also increase, leading to a significantly more intricate cloud security management. This process is also recognized as log management.



IV. CLOUD COMPUTING SECURITY STANDARDS:

A. *Security Assertion Markup Language (SAML):*

Security Assertion Markup Language (SAML) primarily serves business transactions, enhancing secure communication between online entities. This XML-based standard facilitates authentication and authorization across partners. SAML delineates three roles: principal (user), service provider (SP), and identity provider (IDP). Utilizing XML format, SAML queries and responses define user attributes, authorization, and authentication. The inquiring party refers to an internet site receiving security information.

B. *Open Authentication:*

Open authentication is one of the mechanisms for dealing with secure data. It primarily serves as a data access platform for developers. Users can share information with developers and consumers without disclosing their identities. OAuth relies on other protocols, such as SSL, for security.

C. *Open ID:*

OpenID functions as a single-sign-on (SSO) mechanism, providing a unified login approach where users can authenticate once and access all participating systems. Unlike centralized authorization, OpenID does not depend on a central authority to authenticate. Users.

D. *SSL/TLS:*

SSL/TLS, utilized for secure communication over TCP/IP, operates through three distinct phases. Initially, clients negotiate the cipher suites to be employed. Subsequently, key exchange algorithms, utilizing public keys, authenticate the communication in the second phase. Finally, the third phase encompasses message and cipher encryption.

5. CONCLUSION

This article explores cloud principles and qualities, including scalability, Security, reliability platform independence, cost-effectiveness, elasticity etc. This paper discusses security challenges in cloud computing and strategies for preventing them. These techniques can help maintain secure communication and eliminate security issues. The research investigates concerns including attacks, data loss, and unauthorized access to data, along with proposed solutions to mitigate them. This paper introduces cloud computing and its various services. Later, the significance of cloud computing in important businesses. Topics covered include security challenges, cloud computing applications, and future improvements. We have identified multiple security problems, including network and virtualization security. Cloud computing's dynamic and multifaceted nature makes standard security solutions ineffective for virtualized systems. Organizations like the Cloud Security Alliance (CSA) and NIST are focusing on cloud computing security. In this paper, we addressed some of the security measures, although there are several other approaches in the works. Standards are set to provide secure and proper communication and operations in the cloud, where multiple systems interact.

References

[1] G. O Rabi Prasad, Manas Ranjan, Suresh Chandras Cloud “Computing: security issues and Research Challenges” published in IRACSTInternational Journal of Computer Science and Information Technology and Security (IJCSITS), Vol. 1, No. 2, December 2011.

[2] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M, “A view of cloud computing, Communications” of the ACM Magazine, 2010, 53 50-58.

[3] Ashraf I, “An over view of service model of cloud computing” published in Int. J. of Multidisciplinary and Current Research, vol.2, 2014, 779-783.

[4] Bala Narayana Reddy G,” Cloud computing-types of cloud,” 2013, Retrieved from http://bigdatariding.blogspot.my/2013/10/cloudcomputingtypes-of-cloud.html.

[5] Christina A A, “Proactive measures on account hijacking in cloud computing network” published in Asian Journal of Computer Science and Technology, vol.4, 2015, 31-34.

[6] Choubey R, Dubey R and Bhattacharjee J, “A survey on cloud computing security challenges and threats” published in International Journal on Computer Science and Engineering (IJCSE), vol.3, 2011, 1227-1231.

[7] Leonard Kleinrock, “An internet vision: the invisible global infrastructure” published in Ad Hoc Networks, 11, 2003, 1(1):3.

[8] Dinesha H A and Agrawal V K, “Multi-level authentication technique for accessing cloud services” published in International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol.2, 2012, 31-39.

[9] Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D, “Private cloud for collaboration and e-Learning services: from I-a-a-S to S-a-a-S” published in J. Computing-Cloud Computing, 2011, 91 23-42.

[10] Hamlen K, Kantarcioglu M, Khan L and Thurai Singham B, “Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies” published in International Engineering Research and Innovation Symposium (IRIS), IOP Publishing, IOP Conf. Series: Materials Science and Engineering ,160, 012106, vol.8, 2016, 150-162. doi:10.1088/1757-899X/160/1/012106.

[11] Jain S, Kumar R, Kumawat S and Jangir S K, “An analysis of security and privacy issues, Challenges with possible solution in cloud computing”, Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIAIV), 2014, 1-7.

[12] Kandias M, Virvilis N and Gritzalis D, “The insider threat in cloud computing” Proc. of 6th International Conf. on Critical Infrastructure Security, 2011, 95-106.