JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SPECULATIVE ANALYSIS OF CLOUD ARCHITECTURE SECURITY: CHALLENGES AND SIGNIFICANCES

[1]Sujatha. S, [2]Dr. Golam Ambia
[1]Researcher, [2]Professor
[1]Department of Library and Inf. Science, ,
[1] Sunrise University, Alwar, India.

Abstract : Cloud computing has evolved into a crucial component of contemporary IT infrastructure, offering scalable and economical solutions for both businesses and individuals. It fosters collaboration, boosts flexibility, and enables organizations to concentrate on their primary business functions rather than dealing with intricate IT infrastructure management. Cloud computing has an impact on the people, processes, and technology within an enterprise. Despite the advantages associated with the cloud computing paradigm, such as increased efficiency, flexibility, easy setup, and a general reduction in IT costs, it may also introduce concerns related to privacy and confidentiality. Cloud computing relies on the internet as a means for users to access necessary services on a pay-per-use basis at any time. However, despite being in its early stages of development, this technology faces challenges due to threats and vulnerabilities, hindering user trust. Malicious activities from unauthorized users, such as data misuse, rigid access control, and insufficient monitoring, pose significant risks to the integrity of this technology. The presence of these threats can lead to unauthorized or illegal access to critical and confidential user data. The primary objective of this paper is to pinpoint privacy and confidentiality issues that might be of relevance and concern for both participants and users in cloud computing. Therefore, this paper aims to uncover potential problems and regulations within the privacy domain that impact the adoption of Cloud Computing Technologies and propose secure cloud architecture for organizations to strengthen the security.
IndexTerms **- Cloud Computing, vulnerabilities, threats, malicious activity, privacy, confidentiality,Security.**

I. INTRODUCTION

Cloud computing refers to the delivery of computing services, including storage, processing power, and software, over the internet. Instead of relying on local servers or personal devices to handle applications, data storage, and processing, cloud computing allows users to access these resources remotely through the internet. The innovative concept of Cloud Computing introduces dynamically scalable resources delivered as a service over the Internet, offering substantial economic advantages for its adopters. Depending on the nature of the resources provided by the Cloud, distinct layers can be identified and illustrated in figure 1. The lowermost layer supplies fundamental infrastructure components such as CPUs, memory, and storage, commonly referred to as Infrastructure-as-a-Service (IaaS)[1]. An exemplar of IaaS is Amazon's Elastic Compute Cloud (EC2). Above IaaS, there are more platform-oriented services that permit the use of hosting environments customized to specific needs. Google App Engine, for instance, represents a Web platform as a service (PaaS) [2] facilitating the deployment and dynamic scaling of Python and Java-based Web applications. Ultimately, the highest layer furnishes users with readily available applications, commonly referred to as Software-as-a-Service (SaaS)[3]. Two primary technologies are presently discernible for accessing these Cloud services.

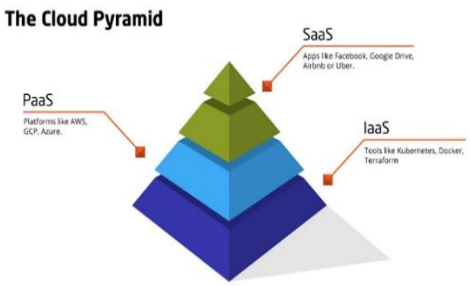

Figure 1: Cloud layers

1.1 Infrastructure as a Service (IaaS)

offers a method of providing a computer infrastructure to a company, typically through platform virtualization. Some companies opt to purchase their own server(s) for hosting their website and services, a solution that can be costly and often requires

additional manpower for maintenance. The server's workload fluctuates, with varying numbers of requests and periods of idle time. If the server remains idle for a significant portion of the time, the company may have invested in a server larger than necessary. Conversely, if the company experiences a sudden surge in popularity and demand, the server may fail due to capacity issues, resulting in a negative impact on the company's reputation. To mitigate such risks, companies can consider purchasing a dedicated server or a web hosting package, which typically involves a fixed monthly fee regardless of server activity or webpage visits. However, with Infrastructure as a Service (IaaS), businesses only pay for the resources they use. Whether the company is small or large, IaaS offers a flexible solution tailored to its specific needs, making it an ideal choice for businesses seeking cost-effective infrastructure solutions [4].

1.2 Platform as a Service (PaaS)

As the array of services available in the cloud continues to expand, the need for an efficient platform to leverage these services becomes evident. Platform as a Service (PaaS) emerges as the provision of an architecture or framework facilitating the growth of cloud computing services. PaaS significantly reduces the cost and complexity associated with evaluating, purchasing, configuring, and managing the hardware and software required for application development [5]. This is achieved by making development tools and delivery tools available within the cloud itself. The key advantage of PaaS lies in the fact that customers are not compelled to invest in expensive hardware or software to develop or utilize applications offered in the cloud.

1.3 Software as a Service (SaaS)

It is a method of delivering software to users via the Internet [6]. The amalgamation of Internet connectivity with software services has been present for a considerable period, although the terminology to describe this phenomenon has only gained clarity in recent years.

The paper aims to enhance awareness within the IT industry regarding the potential of cloud computing by addressing global challenges. It explores various issues that may arise during the implementation of cloud computing. The key objectives include:

- Gathering information and statistics from surveys conducted by reputable organizations.
- Providing a concise overview of security, trust, and privacy concerns in cloud computing.
- Addressing the security challenges encountered by Cloud Service Providers during the implementation of cloud services, presenting mitigation steps, and examining a security model that can potentially resolve some security issues within the cloud environment.

The remainder of the paper is structured as follows: Section 2 delves into related work, providing an in-depth exploration of contributions made by various papers. Section 3 presents a comprehensive overview of cloud computing and discusses general models associated with the cloud. Following this, while Section 4 elaborates on specific cloud security issues and their potential solutions. Moving forward, Section 5 of this survey explores privacy issues in the Context of Third-Party Storagewithin the realm of cloud computing. Finally, the survey concludes in Section 6.

II. RELATED WORKS

The paper [6]provides a comprehensive survey covering cloud architecture and the prevailing security challenges. The primary emphasis is on current security issues within the cloud computing domain. The study explores various security concerns, encompassing communication security, architectural security, and compliance and legal security issues. However, in this paper, the identification is limited to three types of cloud security issues. The document also outlines methods for ensuring secure authentication, authorization, and integrity in web services. Furthermore, it addresses security issues specific to mobile cloud computing. Lastly, the paper delves into several unresolved open issues in the field.

In a study by Balachandra et al in 2009, the focus was on the specification and objectives of security Service Level Agreements (SLAs) pertaining to data locations, segregation, and data recovery [7].

Additionally, Kresimir et al in 2010 addressed overarching security concerns within the cloud computing model, including but not limited to data integrity, payment security, and the privacy of sensitive information [8].

The paper [9] offers a fresh perspective on various types of cloud security issues. The author categorizes each security concern based on the layers of cloud computing and thoroughly examines the issues within each layer. The discussion in the paper provides brief insights into data storage security issues, virtualization security issues, and potential solutions.

The paper [10] delves into the security issues and challenges existing in both public and private clouds. Following this exploration, the authors further examine additional security concerns, including service availability, multi-tenant service issues, data storage issues, and identity and access control issues. Their primary emphasis is on the aspects of data utilization management.

The paper [11] outlines the service model and deployment model of cloud computing. The author's primary focus in this paper is directly on the service model and deployments of clouds. This encompasses discussions on cloud storage architecture, storage as a service, and its associated security requirements. Additionally, the paper delves into the security issues pertaining to cloud storage.

III. TYPES OF CLOUD:

In the context of cloud computing, there are several types of clouds [12], each offering distinct services and deployment models. The main types of clouds are illustrated in figure 2.

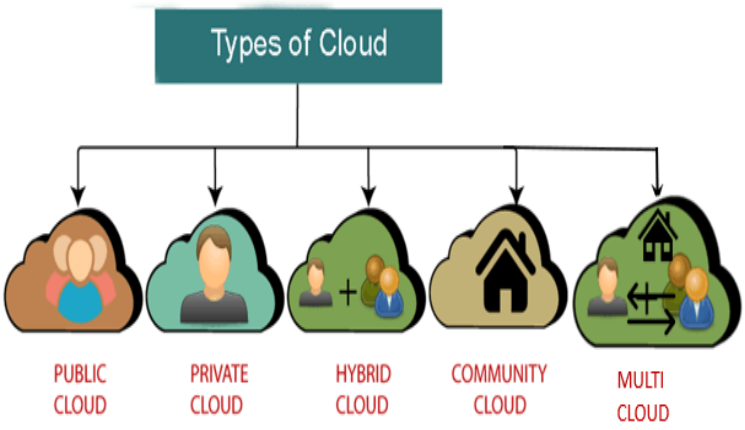

Figure 2: Different types of cloud

3.1 Public Cloud

Definition: Public clouds are owned and operated by third-party cloud service providers. These providers make computing resources, such as servers and storage, available to the general public over the internet.

Characteristics: They are cost-effective, scalable, and accessible to anyone. Users share the same infrastructure, and services are offered on a pay-as-you-go basis.

3.2 Private Cloud

Definition: Private clouds are used exclusively by a single organization. They can be hosted on-premises or by a third-party provider.

Characteristics: Private clouds offer more control, security, and customization compared to public clouds. They are suitable for organizations with specific security and compliance requirements.

3.3 Hybrid Cloud

Definition: Hybrid clouds combine elements of both public and private clouds, allowing data and applications to be shared between them.

Characteristics: Organizations can use the public cloud for scalable and non-sensitive operations while keeping critical workloads in a private cloud. Hybrid clouds provide flexibility and help address specific business needs.

3.4 Community Cloud

Definition: Community clouds are shared by several organizations with common concerns, such as industry regulations or security requirements.

Characteristics: These clouds provide a collaborative platform for multiple organizations while addressing shared concerns. They offer a balance between public and private cloud features.

3.5 Multi-Cloud

Definition: Multi-cloud refers to the use of multiple cloud service providers to meet an organization's requirements.

Characteristics: Organizations may use different cloud providers for specific services or applications. This approach helps prevent vendor lock-in and provides flexibility.

These types of clouds cater to diverse needs and preferences, allowing organizations to choose the model that aligns with their specific requirements, budget constraints, and security considerations.

IV. Prepare Your Paper Before Styling

4.1 Data Security

Upon its creation, data becomes vulnerable to tampering. Improper classification or unauthorized access can occur, leading to a loss of data control. Given that Cloud Service Providers (CSPs) operate as third-party entities, the full security of their systems remains uncertain. Therefore, data must be shielded from unauthorized access, network intruders, and potential leakage [20]. Given the multi-tenant nature of cloud computing, measures must be implemented to address the heightened security risks associated with data co-mingling. Throughout the usage phase, which encompasses transmission between CSP and consumer as well as data processing, confidentiality measures are essential to prevent sensitive data from being compromised through intermingling with network traffic from other cloud consumers. In cases where data is shared among multiple users or organizations, the CSP is responsible for ensuring data integrity and consistency, while also safeguarding all cloud service consumers from malicious activities perpetrated by others. Data persistence poses a significant challenge during the destruction phase. To ensure complete data destruction, it must be properly erased, rendered unrecoverable, and, if applicable, disposed physically.

4.2 Data storage and computing security issues

Data plays a crucial role in the realm of cloud computing, where it is securely stored and shielded from customers' scrutiny. Users are often hesitant to provide their information due to concerns about potential misuse, leading to a constant fear of data falling into the wrong hands. Ensuring the consistency of data during computation, maintaining confidentiality at every processing stage, and perpetually storing data for record updates are paramount considerations.In the context of remote or third-party storage, a significant challenge arises from users' lack of awareness regarding what occurs after their data is stored in the cloud. Data owners are often unaware of the location of the cloud storage center, the security services employed, and the mechanisms used to secure the cloud data [21]. The quality of service becomes a crucial aspect of cloud storage, necessitating proper techniques and mechanisms for efficient and reliable data storage in the cloud.Two distinct situations emerge—before and after the computation of data—each accompanied by various security issues and their corresponding solutions. These issues encompass data storage, untrusted

computing, data and service availability, cryptographic mechanisms, cloud data recycling, and protection against malware.To address these challenges, research is required to develop a system that can consistently, efficiently, and securely store data in the cloud. This would create a trusted environment where individuals feel confident storing their data.

4.3 Recycling of Cloud Data:

Proposing the reuse of cloud space after the proper utilization and disposal of data is a prudent suggestion. However, it is imperative to ensure that data used by a previous user is not accessible to the next user. The process of cleaning or removing specific data from a resource is referred to as sanitization. Following sanitization, refreshed data becomes available for users in a distributed manner [22].Data sanitization is a crucial task in distributed systems to effectively dispose of data and select which data is sent to the garbage. Improper sanitization can lead to data leakage and loss, as the hard disk may delete essential data during the process.

4.4 Access Control:

In the realm of cloud computing, services [23] provided are often critical for users, necessitating a consistently high level of availability. Equally important is ensuring that data stored at cloud hosting sites remains accessible only to the rightful owners of that data. While external customers typically desire exclusive access to their data, it is unavoidable that system administrators overseeing cloud hosting sites also have access. Establishing and maintaining a robust level of trust between the provider and the customer is paramount, just as the cloud computing provider needs to have confidence in the system administrators working for them. Authentication and authorization, achieved through roles and password protection, are commonly employed to maintain access control when accessing cloud computing sites through web browsers. However, a more effective approach to ensuring sufficient security involves implementing an additional authentication factor outside of the browser.

4.5 Key management:

Effective key management [23] poses a critical challenge in cloud infrastructures, given that the virtualization of services obscures the physical location of key storage, rendering traditional protection mechanisms ineffective. Keys are primarily stored and safeguarded at the hardware infrastructure level. In such an environment, deploying tamper-resistant devices for key protection becomes imperative, such as utilizing user smart cards coupled with a Hardware Security Module as integral components of the virtual deployment.

4.6 Adherence to legal and regulatory requirements:

Regulations pertaining to IT security mandate that organizations utilizing IT solutions incorporate specific audit functionalities. However, in the context of cloud computing, organizations leverage services from third-party providers. Existing regulations do not address the audit responsibilities of these third-party service providers. To adhere to audit regulations, organizations establish security policies and implement them through a suitable infrastructure. The security policies set by an organization may impose more rigorous requirements than those mandated by regulations. Bridging any gap between the audit functionality provided by the Cloud Service Provider (CSP) and the necessary audit mechanisms for compliance becomes the responsibility of the cloud service customer [24].

4.7 Cloud Interoperability Issue:

Presently, each cloud service has its own unique approach to how clients, applications, and users engage with the cloud, resulting in the phenomenon known as the "Hazy Cloud." This situation significantly impedes the development of cloud ecosystems, as it enforces vendor lock-in, preventing users from concurrently selecting alternative vendors or offerings to optimize resources across various levels within an organization. The primary objective of achieving interoperability is to facilitate the seamless and fluid exchange of data across clouds and between cloud and local applications. Interoperability is crucial for various levels of cloud computing. Firstly, to optimize IT assets and computing resources, organizations often need to retain in-house capabilities associated with their core competencies while outsourcing peripheral functions and activities to the cloud. Secondly, for the purpose of optimization, organizations may need to outsource various peripheral functions to cloud services offered by different vendors. Although standardization seems to be a viable solution to address interoperability issues, the challenge has not yet become a top priority for major industry cloud vendors as cloud computing is still in its early stages of widespread adoption [25]..

V. PRIVACY ISSUES IN THE CONTEXT OF THIRD-PARTY STORAGE

Data stored with a third party, which includes cloud computing providers, might have less robust privacy protections compared to information held by the original creator. IT managers may be hesitant to relinquish control of their resources to external providers, especially when these providers have the ability to modify the underlying technology without customer consent. Consequently, issues related to performance and latency can be viewed as problematic [26]. Government agencies and private litigants may find it easier to access information from a third party than from the original data creator. The increased capability of government and other entities to obtain information from third parties has implications for both businesses and individuals. For many users, the lack of notification regarding a government demand for data represents a significant reduction in rights.

Web platforms consistently present extensive lists of publications within their terms of service, which may be regarded as the most crucial aspect of cloud computing for an average user not constrained by legal or professional obligations related to privacy and confidentiality[27]-[28]. It is standard practice for a cloud provider to extend its services to users without individual contracts, contingent upon the provider's publicly available terms of service. If these terms grant the cloud provider certain rights over a user's information, the user is likely obligated to adhere to those terms. This has potential implications for the legality of information sharing by a user.

VI. CONCLUSION

While Cloud computing is considered a groundbreaking phenomenon with the potential to revolutionize our Internet usage, exercising caution is essential. A multitude of rapidly emerging technologies brings about significant advancements, offering the potential to enhance human lives. Nevertheless, it is crucial to approach these technologies with careful consideration, fully comprehending the associated security risks and challenges.Cloud computing offers advantages such as rapid deployment, cost efficiency, ample storage space, and convenient system access from any location. Consequently, it has rapidly emerged as a widely accepted computing environment globally. Despite its widespread adoption, security and privacy concerns pose obstacles to the

seamless integration of cloud computing. It is imperative for all cloud users to possess a thorough understanding of the vulnerabilities, threats, and potential attacks present in the cloud. Increased awareness of these security challenges can facilitate organizations in achieving swift adoption of cloud computing. The utilization of both traditional and innovative technologies in cloud computing introduces specific security issues associated with this emerging technology landscape.

REFERENCES

[1] Ashish Singh, Kakali Chatterjee, "Cloud security issues and challenges: A survey",Journal of Network and Computer Applications, Volume 79, Pages 88-115,(2017).

[2] Ajmal, A., Ibrar, S., & Amin, R. (2022). Cloud computing platform: Performance analysis of prominent cryptographic algorithms. Concurrency and Computation: Practice and Experience. https://doi.org/10.1002/cpe.6938.

[3] Raza, S. M., Ahvar, S., Amin, R., & Hussain, M. (2021). Reliability aware multiple path installation insoftware-defned networking. Electronics, 10, 2820.

[4]Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015 Jun 1;305: pp. 357-383.

[5] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues inCloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009pp 110-112.

[6] M. Ali et al.Security in cloud computingopportunities and challengesInf. Sci.(2015).

[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC'09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[7] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROCThird International Conference on Advances in Human-oriented and PersonalizedMechanisms, Technologies, and Services, 2010, pp. 344-349.

[8] Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing. 2013 Feb 1;63(2): pp. 561-592.

[9] Tari Z., Yi X., Premarathne U. S., Bertok P., and Khalil I. Security and privacy in cloud computing: Vision, trends, and challenges. Cloud Computing, IEEE, vol. 2, no. 2, pp. 30-38, 2015.

[10] Kulkarni G, Waghmare R, Palwe R, Waykule V, Bankar H, Koli K. Cloud storage architecture. InTelecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on 2012 Oct 30 (pp. 76-81). IEEE.

[11] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing:Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing andCommunications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[12] Xiaojun Yu; Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle," ComputationalIntelligence and Software Engineering (CiSE), 2010 International Conference on , vol., no., pp.1-4, 10-12Dec. 2010.

[12] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEEInternational Conference on Web Services, pp. 607-616. July 2009.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An EnterprisePerspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[14] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Gridand Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43,2010.

[15] Puthal, Deepak, B. P. S. Sahoo, Sambit Mishra, andSatyabrata Swain. "Cloud Computing Features, Issues andChallenges:A Big Picture." 2015 International Conference onComputational Intelligence & Networks. Odisha, India: IEEE,2015. 116-123.

[16] Dinadayalan, P., S. Jegadeeswari, and D. Gnanambigai. "DataSecurity Issues in Cloud Environment and Solutions." 2014World Congress on Computing and CommunicationTechnologies. Trichirappalli, India: IEEE, 2014. 88-91.

[17] Erdogmus, H.: Cloud Computing: Does Nirvana Hide behind the Nebula?IEEE Software. 26 (2) (2009) 4–6.

[18] Vaquero,L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A Break inthe Clouds: Towards a Cloud Definition. ACM SIGCOMM ComputerCommunication Review. 39(1) (2009).

[19] Hayes, B.: Cloud computing. Communications of the ACM. 51 (7) (2008).

[20] Grossman,R.L.,: A quick introduction to Clouds. Open Data Group.Technical Report No. 1, 2008.

[21] Singh and Dalal (2010), In Absence of Dedicated Privacy Law & Data Protection Law - Is IndiaReady for Cloud Computing? http://www.techno-pulse.com/2010/12/privacy-data-protectionlaw-india-cloud.html

[22] Sultan, N. (2010), Cloud computing for education: A new dawn? International Journal ofInformation Management, Volume 30, Issue 2, April 2010, Pages 109–116.

[23] Weinhardt C., A. Anandasivam, B. Blau and J. Stosser (2009), Business Models in the ServiceWorld, IT Professional, Vol. 11 No 2, pp. 28-33 .

[24] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues inCloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009pp 110-112.

[25] N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, pp. 15-20, 2009.

[26] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues inCloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.

[27] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure CloudComputing", Wiley Publishing, Inc.,2010.

[28] Kuyoro S. O, Ibikunle F and Awodele O, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) (2011).