e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

REVIEW ON CLOUD COMPUTING ARCHITECTURE AGAINST ISSUES AND CHALLENGES

Ankita Sharma Rajoriya*1, Dr. Vinod Sharma*2
SGSU, India.

ABSTRACT

Cloud Computing services need to address the security during the transmission of sensitive data and critical applications to shared and public cloud environments. The cloud environments are scaling large for data processing and storage needs. Cloud computing environment have various advantages as well as disadvantages on the data security of service consumers. Cloud computing is based essentially on platforms and servers virtualization and promises the reduction of costs and the increase of flexibility. This paper review on all patterns of different cloud architecture and services. In this paper, we propose a cloud computing architecture offering the ease of resources management, access security and service availability in a reliable structure with lower cost.

Keywords: Cloud Computing; Security and Privacy; Threats, Vulnerabilities, Secure Cloud Architecture.

I. INTRODUCTION

Prior to cloud computing, organizations spent days, weeks and sometimes months to provision new servers for projects, new systems, software upgrades, performance and scalability reasons. This process was extreme long because IT departments needed to order new hardware, and the hardware vendors would take days to prepare and ship them, the shipment will take a few days to arrive, then the IT team need to register, image and configure the new servers, and finally it will be handed over the appropriate team that requested them. This would take at least a week or two depending on the urgency; in larger organizations with more bureaucracy this might take 2-6 months to fulfill similar requests.

Because of the above delays and limited flexibility, the Technology Industry and businesses have been craving for ways to utilize high power and on-demand computing along. Because of these needs, computing has evolved from a single operating system per hardware, to virtualization (single hardware multiple operating systems) and now it has advanced to cloud computing (on-demand computing as services and no hardware required).

Types of cloud services and architecture models Since cloud technologies are addressing a wide range of demands, delivering a one-size-fit-all solution would not have worked, because every organization is different from the other in multiple ways. In this section, we will discuss the different layers of cloud services as well as their deployment models.

Because cloud computing is more than just hosting an organization's information system at a network location, it encompasses prebuilt services not otherwise available in a traditional data center. Therefore, it has evolved to handle the diverse needs of the different consumers and businesses who need the service. The cloud services can be divided into two major categories, namely the Deployment Model and Service Model.

Deployment Model includes:

Private Cloud :-

In this deployment model, the cloud environment is hosted exclusively for a particular organization either on premise or off premise, and it can be managed by the organization or a third party.

An example of this deployment model could include: an organization installing OpenStack, CloudStack or other cloud like management services to convert an existing data center into a cloud environment.

This can be used by large organizations that already have a well-established IT Department with a lot of critical applications and data.

Hybrid Cloud

This is a composition of two or more cloud environments that remain separate entities but are connected through proprietary technologies to enable them to seamlessly share data and applications through a standardized process,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

This model is a lot more secure, because the organization can use their traditional security policies and network architecture to properly isolate, manage, and control their IT Infrastructure.

Community Cloud

In this deployment model, the cloud infrastructure or platform is shared by a specific group of organizations with common objectives or mutual concerns. This isolated and shared system is on a dedicated hardware and can be hosted by one of the organizations, or a third party provider.

Public Cloud

In this deployment model, the cloud services are made available to the general public, businesses and large institutions, and it is owned and operated by a Cloud provider who sells the services as a utility for consumption.

II. RESEARCH METHODOLOGY

With Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has become important issues to highlight. There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers.

2.1 Proposed Work Explanation

Day by day performance of cloud architecture & services are increases. Performance testing is a testing measure that evaluates the speed, responsiveness and stability of a computer, network, software program or device under a workload. Organizations will run performance tests to identify performance-related bottlenecks.

The goal of performance testing is to identify and nullify the performance bottlenecks in software applications, helping to ensure software quality. Without some form of performance testing in place, system performance may be affected by slow response times and inconsistent experiences between users and the operating system.

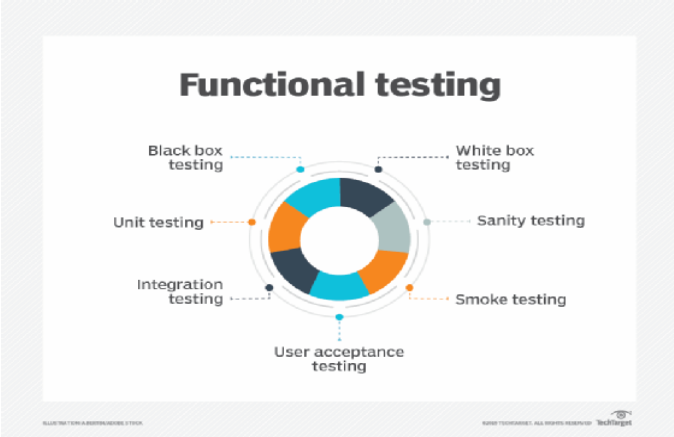

Figure 2.1 Diagram on functional testing

2.2 Cloud performance testing

Developers can carry out performance testing in the cloud as well. Cloud performance testing has the benefit of being able to test applications at a larger scale, while also maintaining the cost benefits of being in the cloud.

At first, organizations thought moving performance testing to the cloud would ease the performance testing process, while making it more scalable. The thought process was they could offload the process to the cloud, and that would solve all their problems. However, when organizations began doing this, they started to find that there were still issues in conducting performance testing in the cloud, as the organization won't have in-depth, white box knowledge on the cloud provider's side.

One of the challenges with moving an application from an on-premises environment to the cloud is complacency. Developers and IT staff may assume that the application works the same once it reaches the cloud. They might minimize testing and quality assurance, deciding instead to proceed with a quick rollout. Because the application is being tested on another vendor's hardware, testing may not be as accurate as on-

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

premises testing. Development and operations teams should check for security gaps; conduct load testing; assess scalability; consider UX; and map servers, ports and paths.

Interapplication communication can be one of the biggest issues in moving an app to the cloud. Cloud environments typically have more security restrictions on internal communications than on-premises environments. An organization should construct a complete map of which servers, ports and communication paths the application uses before moving to the cloud. Conducting performance monitoring may help as well.

2.3 Performance testing challenges

Some challenges within performance testing are as follows:

- Some tools may only support web applications.
- Free variants of tools may not work as well as paid variants, and some paid tools may be expensive.
- Tools may have limited compatibility.
- It can be difficult for some tools to test complex applications.
- Organizations should watch out for performance bottlenecks in the following:
  - CPU.
  - Memory.
  - Network utilization.
  - Disk usage.
  - OS limitations.
- Other common performance problems may include the following:
  - Long load times.
  - Long response times.
  - Insufficient hardware resources.
  - Poor scalability.

III. SERVICE PROVIDER SECURITY ISSUES

The public cloud computing surroundings offered by the cloud supplier and make sure that a cloud computing resolution satisfies organizational security and privacy needs. The cloud supplier to provision the safety controls necessary to safeguard the organization's information and applications, and additionally the proof provided regarding the effectiveness of these controls migrating organizational information and functions into the cloud.

3.1 Identity and access management

Identity and Access Management (IAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any organization "trust boundary" is mostly static and is monitored and controlled for applications which are deployed within the organization's perimeter. In a private data center, it managed the trust boundary encompasses the network, systems, and applications. And it is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication.

With cloud computing, the organization's trust boundary will become dynamic and the application, system, and network boundary of an organization will extend into the service provider domain. Application security and user access controls will compensate for the loss of network control and to strengthen risk assurance. Strong authorization, authentication based on claims or role, trusted sources with user activity monitoring, identity federation , accurate attributes, single sign-on (SSO), and auditing.

3.2 Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In Private and confidential customer data fast rising for the consequences and potential costs of mistakes for

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal issues.

3.3 Securing Data in Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

3.4 User Identity

In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privilegeduser monitoring, including logging activities. This monitoring should include background checking and physical monitoring. To coordinate authentication and authorization with the enterprise back-end or third-party systems are identity federation and rapid on boarding capabilities. For allowing users to easily and quickly leverage cloud services use single sign-on capability is required to simplify user logons for both the cloud and internally hosted applications.

3.5 Audit and Compliance

An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail. In traditional Out sourcing relationships plays an important role for Audit and compliance. In Cloud dynamic nature, increase the importance of these functions in platform-as-aservice (PaaS), infrastructure-as-a-service (IaaS), and software-as-a-service (SaaS) environments. Customers' business and regulatory requirements are monitor ,establish and demonstrate with set of controls and it is a challenge task for Cloud service providers (CSPs). In clouds , to audit and compliance with coordination of external auditing, regulatory compliance and internal policy compliance.

3.6 Cloud Integrity and Binding Issues

In a Cloud Computing system, the major responsibility is coordinating and maintaining instances of virtual machines (IaaS) or explicit service execution modules (PaaS). For any user request, the Cloud system is responsible for determining a free-to-use instance of implementation type for the requested service and for accessing that new instance the address is to be communicated for the requesting user. Cloud Malware Injection Attack is a basic attack in Cloud system for attempt aims at injecting a malicious service performance or virtual machine. It is useful for any purpose the adversary is interested in data modifications to full functionality changes or blockings. This attack requires to adding to the Cloud system by creating its own malicious service implementation module (PaaS or SaaS) or virtual machine instance (IaaS).

3.7 Flooding Attacks

Cloud system provider maintains all basic operational tasks in Cloud Computing. In this tasks server hardware maintenance is the most important instead of operating as own hardware. So, Cloud Computing enables companies (clients) to rent server hardware on demand (IaaS). It gives more economic benefits when it comes to dynamics in server load. Same servers can operate in different time zones with different data traffic. In Cloud Computing environment provides a dynamic adaptation of hardware requirements to the actual workload

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

occurring without buying sufficient server hardware for the high workload times. Practically, it can be achieved by using virtual machines. If a company's demand on computational power rises, it simply is provided with more instances of virtual machines for its services. Direct Denial of Service is a service attack involves saturating the objective with bogus requests to prevent it from responding to reasonable requests in a timely manner. An attacker to launch physical attack typically uses multiple computers or a botnet. It can capture large number of resources to protect against and cause charges to rise. The cloud dynamic provisioning in some ways minimizes the task of an attacker to cause harm. At the same time, the resources of a cloud are significant with enough attacking computers they can become saturated. Indirect Denial of Service is manage the computational power of the attacker, in cloud service the direct flooding attack gives some side effect and the same hardware provides some other services may suffer the workload caused by the flooding. The service instance may on flooded service instance, the same server with another. By using the flooding attack requests the server's hardware resources are completely exhausted, then the same hardware machine are unable to perform the other service instances intended tasks. So, the Denial of Service is targeted other services with target service instances on the same server hardware. In Cloud computing environment, denial of service can cause and notice the lack of availability and switch to other service instances to other servers. It is extra burden to all other servers and it spreads all the servers in the complete computing Cloud.

3.8 Accounting and Accountability

Accounting and Accountability is a main cost-effective driver behind operation a Cloud Computing service is charging the customers according to their actual usage and another flooding attack on a Cloud service is drastically increasing the bills for Cloud usage. For computational power usage there is no "upper limits" then the client running the flooded service most likely has to foot the bill for the workload caused by the attacker.

IV. CHALLENGES IN CLOUD COMPUTING

Cloud is an important resource with its various benefits, but it has various risks and challenges as well. This article will dive deep into a few of the most common cloud computing challenges faced by the industry, cloud security challenges and risks, and cliched cloud computing problems and solutions.

The top 12 cloud computing challenges are:

Figure 4.1 Cloud Computing Challenges

4.1 Data security and privacy

When working with Cloud environments, data security is a major concern as users have to take responsibility for their data, and not all Cloud providers can assure 100% data privacy.

No identity access management, lack of visibility and control tools, data misuse, and cloud misconfiguration are the common reasons behind cloud privacy leaks. There are also concerns about malicious insiders, insecure APIs, and neglect or oversights in cloud data management.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Solution:

Install and implement the latest software updates, as well as configure network hardware to prevent security vulnerabilities. Using antivirus and firewalls, increasing bandwidth for Cloud data availability, and implementing cybersecurity solutions are some ways to prevent data security risks.

4.2 Multi-cloud environments

Multi-cloud environments present issues and challenges such as – configuration errors, data governance, lack of security patches, and no granularity. It is difficult to apply data management policies across various boards while tracking the security requirements of multi-clouds.

Solution:

Implementing a multi-cloud data management solution can help you manage multi-cloud environments. We should be careful while choosing the solution, as not all tools offer specific security functionalities, and multi-cloud environments continue to become highly sophisticated and complex.

4.3 Performance challenges

The performance and security of cloud computing solutions depend on the vendors, and keep in mind that if a Cloud vendor goes down, you may lose your data too.

Solution:

Cloud Service Providers should have real-time SaaS monitoring policies.

4.4 Interoperability and flexibility

When you try to shift applications between two or multiple Cloud ecosystems, interoperability is a challenge. Some of the most common issues are:

- Match the target cloud environment's specifications by rebuilding application stacks
- Managing services and apps in the target cloud ecosystem
- Working with data encryption during migration
- Configuring networks in the target cloud for operations

Solution:

Before starting work on projects, setting Cloud interoperability as well as portability standards can help organizations solve this problem. The use of multi-layer authorization and authentication tools is a good choice for account verifications in hybrid, public, and private cloud ecosystems.

4.5 High dependence on network

When transferring large volumes of information between Cloud data servers, a lack of sufficient internet bandwidth is a common problem. There is a risk of sudden outages, and data is highly vulnerable. To help prevent business losses from sudden outages, enterprises should ensure there is high bandwidth without sacrificing performance.

Solution:

Focus on improving operational efficiency and pay more for higher bandwidth to address network dependencies.

4.6 Lack of knowledge and expertise

Hiring the right Cloud talent is another common challenge in cloud computing. There is a shortage of working security professionals with the necessary qualifications in the industry. As the workloads are increasing, so are the number of tools launched in the market. Enterprises need good expertise in order to efficiently utilize these tools and look out for the best fit.

Solution:

Hire Cloud professionals having specializations in DevOps as well as automation.

4.7 Reliability and availability

High unavailability of Cloud services, as well as lack of reliability, are the major concerns in these ecosystems. In order to keep up with ever-changing business requirements, businesses are forced to seek additional computing resources.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

If a Cloud vendor gets hacked, the sensitive data of organizations using their services gets compromised.

Solution:

Improve both aspects by implementing the NIST Framework standards in Cloud environments.

4.8 Password security

Account managers manage all their cloud accounts using the same passwords. Password management poses a critical problem, and it is often found that users resort to using weak and reused passwords.

Solution:

Secure all your accounts by using a strong password management solution. To further improve security, in addition to a password manager, use Multifactor Authentication (MFA). Cloud-based password managers should alert users of security risks and leaks.

4.9 Cost management

Although Cloud Service Providers (CSPs) offer a pay-as-you-go subscription model for services, hidden costs are charged as underutilized resources in enterprises, making the costs can add up.

Solution:

Implementing resource utilization monitoring tools as well as auditing systems regularly are some ways organizations can fix this. It's one of the most efficient methods to deal with major challenges and manage budgets in cloud computing.

4.10 Lack of expertise

Cloud computing is a highly competitive field, and there are many professionals who lack the required knowledge and skills to be employed in the industry. There is also a huge gap in supply and demand for certified individuals and many job vacancies.

Solution:

Companies should help existing IT staff in upskilling their careers and skills by investing in Cloud training programs.

4.11 Control or governance

Good IT governance makes sure that the right tools are used and assets get implemented as per procedures and agreed-on policies. Lack of governance is a common problem in cloud computing, and companies utilize tools that do not align with their vision. IT teams don't get total control of compliance, data quality checks, and risk management, thus creating many uncertainties when migrating to the cloud from traditional infrastructures.

Solution:

Traditional IT operations should be adopted to accommodate Cloud migrations.

4.12 Compliance

When it comes to having the best data compliance policies, cloud Service Providers (CSP) are not up-to-date. Organizations run into compliance issues with state laws and regulations whenever a user transfers data from internal servers to the cloud.

Solution

The General Data Protection Regulation Act is expected to address compliance issues in the future for CSPs.

V. CONCLUSION

While cloud computing provides lower Infrastructure cost, higher agility and faster delivery, it also presents higher operational and security risks for business critical assets, but a well-designed solution and security architecture will keep businesses safe during and after migrating their assets to the cloud. This paper will research and identify best security practices and how to improve a security architecture in an enterprise cloud environment. It will also review some of the cloud vendors practice statements, other cloud research literature, cloud reference architecture and other cloud security frameworks. Cloud computing was found to have some high security risk and higher operations cost associated with it. But above mentioned solution are provide better & secure environment to a cloud architecture,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

VI. REFERENCES

[1] V.KRISHNA REDDY1 , Dr. L.S.S.REDDY "Security Architecture of Cloud Computing "International Journal of Engineering Science and Technology (IJEST).2017

[2] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing.

[3] Michael Gregg, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Global Knowledge, 2010.

[4] A Khaldi, K Karoui, N Tanabè " A Secure Cloud Computing Architecture Design" 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.

[5] Mell, P. Grance, T., 2011, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145 (Draft). Retrieved 2013-10-11)

[6] M. Grimes, P. T. Jaeger and J. Lin, " Weathering the Storm: The Policy Implications of Cloud Computing", 2009, [Accessed: 19- Jul-2011].

[7] KashifMunir and SellapanPalaniappan, "SECURE CLOUD ARCHITECTURE", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013, [Accessed: 13-05- 2013].

[8] Kashif Munir and Prof Dr. Sellapan Palaniappan "Secure Cloud Architecture" Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013.

[9] Abed, AK & Anupam, A 2022, Review of security issues in internet of things and artificial intelligence driven solutions, Security and privacy, vol. 6, no. 3, pp. 285-300.

[10] Bokefode, JD, Bhise, AS, Satarkar, PA, & Modani, DG 2016, Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption, Procedia Computer Science, vol. 89, no. 2, pp. 43-50.

[11] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing.

[12] Stephen C. Hawald , Cloud Computing with Software as a Service (SaaS): How It Is Changing the Business and Organization Today, IT Today.

[13] https://www.researchgate.net/publication/27619 6135_Secure_Cloud_Architecture.

[14] http://www.esearchgate.net/publication/327010324_Cloud_Security_Architecture_and_Implementation_-_A_practical_approach.

[15] https://scholar.google.co.in/scholar?q=researchpapers on cloud security architecture in cloud computing & hl=en & as_sd t=0 & as_vis =1 & oi = scholar.