iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** II **Month of publication:** February 2023

DOI: https://doi.org/10.22214/ijraset.2023.48994

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

A Study of Virtualization Techniques Applied in Cloud Computing Environment

Neha Kumari[1], Dr. Uday Narayan Singh[2]
[1]*Research Scholar Magadh University, Bodh-Gaya*
[2]*Associate Prof. & Head Dept. of Physics, K.S.M. College, Aurangabad (Bihar)*

Abstract: ***The fastest-growing internet technology today is cloud computing. On-demand network access to a shared pool of reconfigurable resources is possible. A fundamental component of cloud computing is virtualization, which enables real resources to be divided into virtual resources so they can be shared among other virtual machines. Utilizing this virtualized resource can help you use less real equipment, servers, and storage space.***
Modern technologies like cloud computing expand the functional possibilities, elastic resource management, and collaborative execution style of applications. Virtualization, which enables business or academic IT resources through on-demand allocation dynamically, is the core component of cloud computing. The resources come in a variety of shapes, including client, server, storage, network, and application. This essay focuses on how virtualization increases the resources' elasticity in a cloud computing context. This study also provides a thorough analysis of open source virtualization approaches, problems, and future research directions.
Keywords: Hypervisor ,Virtualization, Cloud Computing, Virtual Machine, Virtual Machine Monitor (VMMs), containerization ;

I. BACKGROUND

The IT giant IBM launched a project named CP/CMS (Control Program / Cambridge Monitor System) System in 1964, which is when the virtualization techniques were first developed. An operating system called the Control Program has the ability to use a machine's physical computing resources in many virtual forms. This was an operating system or time-sharing application that later developed into a virtual machine. At first, virtual resources were either employed in the same location or in specialized computing resources as requested by the intended organization. However, they were not available in self-service or on-demand modes at the time. Virtual copies of computer and network resources did exist at the time.
Today, the cloud uses virtualization techniques to generate pools of resources and administer them in the form of virtual computers. These resources are then made available to users and clients in self-service mode over the Internet or Intranet. The IT market now offers a variety of VMware products that may be used to generate and replicate virtual resources. Some of them are unrestricted, while others can be acquired legally.

II. INTRODUCTION TO THE TOPIC

Technology called cloud computing enables users to access a lot of computing resources. Individuals and organizations can forego investments and merely employ the resources already at their disposal. Pay-per-use is used in this process. A virtual machine, as it relates to virtualization, is a machine inside a machine that doesn't actually exist in the real world. It can also have its own OS and offer user applications. Because of significant cost reductions and enhanced management, virtualization is becoming more and more common in enterprise cloud computing settings. Resource sharing and server consolidation are the end results.
A collaborative IT (Information Technology) environment known as "the cloud" is designed with the goal of measuring and remotely delivering scalable IT resources for effective and efficient utilization. A definition of cloud computing provided by the National Institute of Standards and Technology (NIST) reads as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with little management effort or service provider interaction[1]."
Hardware, a hypervisor, and a virtual machine monitor are the components of virtualization approaches (VMM). It permits the dynamic allocation of intellectual IT resources such as network, storage, application, server, and client on demand. In order to improve system security, flexibility, scalability, and dependability, this hypervisor becomes important. Enterprises have expressed a growing interest in using virtualized systems in recent years, mostly to cut costs and use resources more effectively.

In this study, various hypervisor and virtualization approaches are discussed, along with how they contribute to the expansion of resource elasticity in a cloud computing context [2].

Hardware isolation, encapsulation, and independence are all features of virtual computers. Disaster recovery, testing, training, product evaluations, quality assurance, software development, shorter provisioning times, improved security, server consolidation, higher hardware utilization, and finally, easier administration tasks are all advantages of virtualization.

On-demand self-service, broad network access, resource pooling, quick elasticity, and measured service are the five fundamental aspects of cloud computing that NIST lists. Anytime, anywhere access to programmes and data via the internet via mobile devices is referred to as mobile cloud computing. Traditional computing resources are kept in a single device and accessed by a user who has provided authentication. In cloud computing, resources are centrally stored and retrieved as needed. Mobile devices and subsequent mobile computing have recently emerged as essential elements of cloud computing.

III. VIRTUALIZATION

A key technology in the cloud computing environment is virtualization. It offers two crucial properties, encapsulation and abstraction [1]. Between hardware and software, an abstract layer is to be created. The virtualization layer of the Cloud's architecture is typically positioned above the physical layer. Due to the advantages it provides, such as better resource utilization, lower costs, simpler server management, server consolidation, and live virtual machine migration, virtualization technology is widely used in cloud computing data centers.

Through virtualization, the quantity of hardware resources used in clouds can be decreased, lowering capital costs as well as costs associated with cooling and power consumption. For instance, numerous (virtual) servers may be permitted to operate concurrently on a single physical server through server consolidation. Additionally, live migration of the virtual machine to the underutilized physical servers would permit an increasing number of physical servers to be turned off, improving data centers' ability to achieve energy efficiency.

IV. VIRTUALIZATION IN CLOUD COMPUTING

The cloud computing virtualization can suggest dynamic configurations for various application resource requirements and combine these resources for various uses. By automatically monitoring, maintaining, and provisioning resources, it can also increase responsiveness. It makes it possible to gain the advantages of virtual machines, which can increase scalability in addition to providing other benefits like security, cost effectiveness, etc. The primary goal of virtualization is to jointly utilize IT resources, such as storage, processors, and networks, to their fullest extent while lowering the cost of IT resources. This can be accomplished by combining multiple idle resources into shared pools and by creating various types of virtual machines to perform various tasks concurrently. The resources can be dynamically allocated or changed.

The virtualization splits the physical Information Technology Resources into multiple physical objects that can be executed over the various separate operating systems. The cloud architecture separates and hides these services to deliver the on-demand and specialized services to the cloud users.

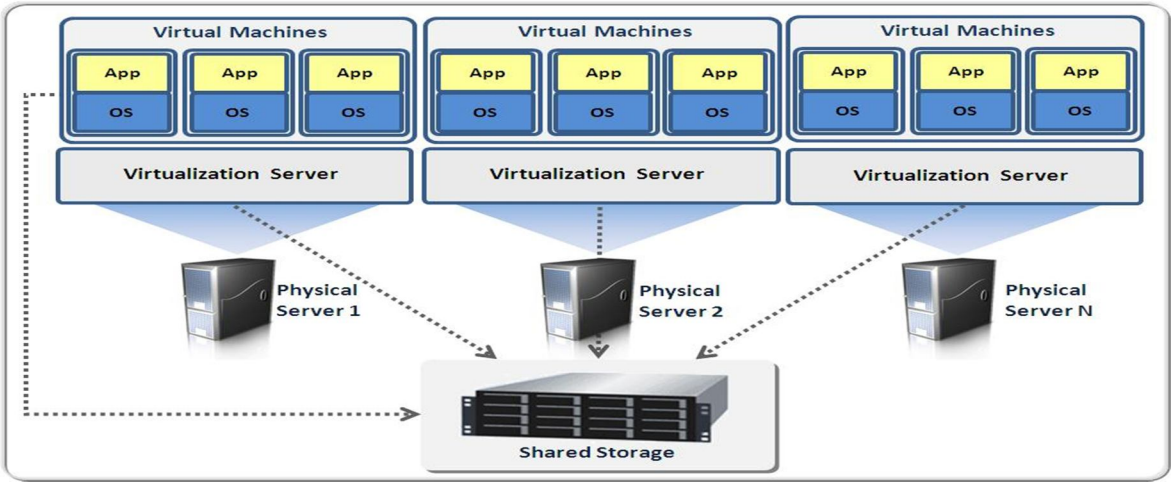


Fig. 1: Architecture of Virtualization

Source: https://www.researchgate.net/figure/illustration-of-the-concept-of-Virtualization-7_fig1_269636339

The use of logical rather than physical IT resources is now the human perspective as a result of virtualization technologies [3] [4]. Virtualization aims to maximize the cooperative use of IT resources like storage, processors, and networks while lowering the cost of those resources. This can be done by grouping idle resources into shared pools and setting up many virtual computers to carry out diverse activities at once. The resources can be dynamically distributed or changed. When using virtualization in a cloud computing environment, the user needs be aware of fundamental approaches such as emulation, hypervisor, full, para, and hardware aided virtualization. The major techniques applied for virtualization in cloud computing environment are:

1) *Hypervisor or VMM:* It is a layer of software capable of managing and virtualizing a host machine's resources in accordance with user needs [5]. It is a layer in between the operating system and the hardware. Hypervisors can be broadly categorized as native and hosted [6]. While host-based hypervisors run on the host operating system, native-based hypervisors run directly on the hardware. Virtual resources such as CPU, memory, storage, and drivers are created by the software layer.
2) *Emulation:* It is a virtualization technique found in the operating system layer that resides on the hardware and transforms the behavior of the computer hardware into a software program. While emulation offers a great deal of flexibility to the guest operating system, it does so at a lower translation speed than a hypervisor and with a higher configuration of hardware resources [7].
3) *Para Virtualization:* This method offers unique hyper-calls that can replace the host machine's instruction set architecture. In order to increase effectiveness and performance, it relates communication between the hypervisor and the guest operating system. Since all resources must be simulated in a full virtualization model, accessing resources is better with para-virtualization [8]. The disadvantage of this method is that it uses hyper-calls to alter the kernel of the guest operating system. Only open source operating systems can use this model.
4) *Full Virtualization:* The host or server hardware and the virtual server are placed in an isolated environment thanks to the hypervisor. Without taking into account the virtualized environment or need changes, operating systems directly contact hardware controllers and its peripheral devices [9].

V. TYPES OF VIRTUALIZATION

Server virtualization, client virtualization, and storage virtualization are the three main types of virtualization.

1) *Server Virtualization:* In server virtualization, a single server handles the work of numerous servers by distributing its resources across various environments. The hypervisor layer enables the local or distant hosting of several programmes and operating systems. Cost reductions, decreased capital expenses, high availability, and effective resource use are just a few benefits of virtualization.

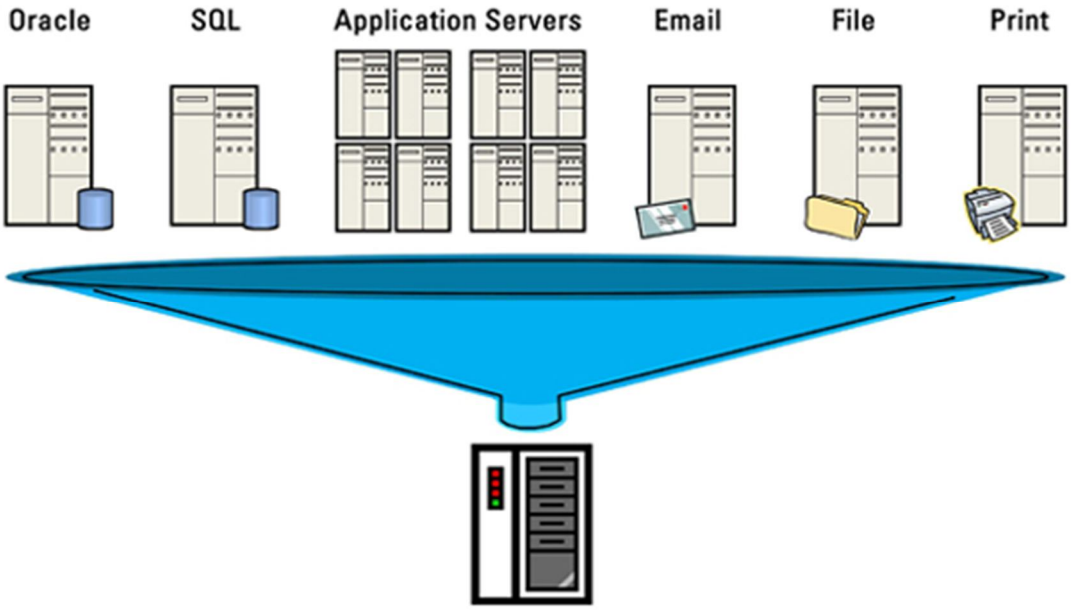


Fig. 2: Server Virtualization
Source:https://www.energystar.gov/products/low_carbon_it_campaign/12_ways_save_energy_data_center/server_virtualization

2) *Client or Desktop Virtualization:* The system administrator may virtually update and monitor client workstations like desktop, laptop, and mobile devices thanks to client virtualization technology. It optimizes client machine administration and security to protect against hackers and online criminals. Client virtualization comes in three different varieties. First, remote or server-hosted virtualization, which is run by the client through a network and is hosted on a server machine **[10]**. The second type of virtualization is local or client-hosted, in which the virtualized and secure operating environment runs on a local machine. Third, there is application virtualization, which offers a variety of non-traditional ways to run an application **[11]**. In this method, a programme is operated in a separate virtualized environment or through the use of partitioning.

Fig. 3: Client Virtualization

3) *Storage Virtualization:* It makes it possible to isolate logical storage from physical storage. DAS (Direct Attached Storage), NAS (Network Attached Storage), and SAN are the three types of data storage that are utilized in virtualization (Storage Area Network). The standard technique of data storage, or DAS, involves directly connecting storage discs to the server system. NAS is a shared storage system that connects via a network. The NAS is utilized by machines for file sharing, device sharing, and backup storage. SAN is a storage system that is shared by numerous servers across a fast network. The software package known as a hypervisor manages functioning access to the host machine's physical hardware. Hosted and bare metal/native hypervisor models are the two different types. While bare metal based hypervisors run directly on the host machine's hardware, hosted hypervisor instances run on top of the host operating system.

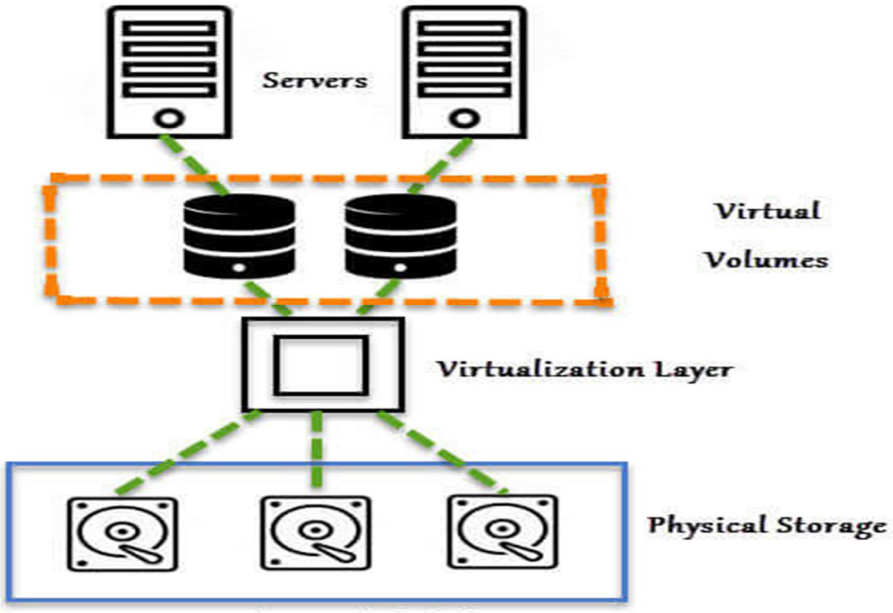


Fig. 4: Storage Virtualization
Image Source: “https://www.storagetutorials.com/”

VI. MAJOR OBSTACLES

The majority of challenges facing virtualization and cloud computing are related to fundamental management issues such data leakage, virtualization security risks, data persistence problems, privacy, and elastic resource management.

1) *Leakage of Data:* When an employee secures access to an organization's data that is kept in a cloud system, there is a high danger of data leakage. Data leaks **[12]** are caused by unsafe multitenant environments at the hypervisor level, unsecure remote access, third-party storage, and hacking of data locations. To prevent data leakage, a cloud provider or broker can improve the prevention and detection system and create a cooperative security policy at the hypervisor level.
2) *Security Threats in Virtualization:* Virtual machine, hypervisor, virtual infrastructure, and virtual network threats are the several types of security risks associated with virtualization **[13]**. When processing virtual machine status, software updates, resource competition, patching, and virtual machine conurbation, the threat to virtual machines emerges. The Virtual-Machine-Based Root-kit (VMBR) assault and the Blue Pill Attack **[14]** are pinned by the hypervisor threat, which is essential to virtualization. Physical access and single point of control are the main challenges to virtual infrastructure. The security tools of intrusion detection, preventive mechanisms, virtual switches, and networks corresponding to the needs can effectively address virtual network threats.
3) *Data Lifetime Concern:* Once a piece of data has served its purpose, it will be securely erased so that malicious users cannot recover it. As is customary, a corporation has complete control over the servers that house the utilized data **[15]**. However, with cloud computing, end users and cloud users do not have secure delete access to the physical cloud provider equipment. The cloud provider should pay close attention to prevent data recovery by nefarious users. referring to the demands.
4) *Privacy Concerns:* Data stored in the data centers of cloud service providers that are geographically dispersed raises serious privacy concerns for cloud customers **[16]**. There are various conditions in the cloud that put users' privacy at risk. First, there are storage problems that arise when data is stored in several places that are concealed from the user and have the potential to be transferred without the owner's consent. The second main worry is making sure that the cloud provider, broker, and user have a destruction time policy in place once the data has reached its expiration date. The third issue is data breaches, which include research on how they happen and who would be held accountable if a data breach occurs in the cloud. When choosing to use cloud services, a user should carefully understand the terms and conditions before proceeding. The fourth issue is with regular policies for auditing and monitoring. To ensure that their stakeholder personal information is not compromised while cloud resources are being shared with others, cloud clients should continuously monitor and audit the operations of the cloud service provider.
5) *Elastic Resource Management Issues:* The system clusters and large volume of data created by cloud computing systems result in new issues. We must consider challenges like resource allocation, provisioning, mapping, and adaptability in order to implement successful elastic resource management. The requirements for service level elasticity and availability are problematic for cloud services. Through the application of efficient elastic resource management strategies, the high performance of the cloud may be accomplished, allowing users to receive effective services from service providers.

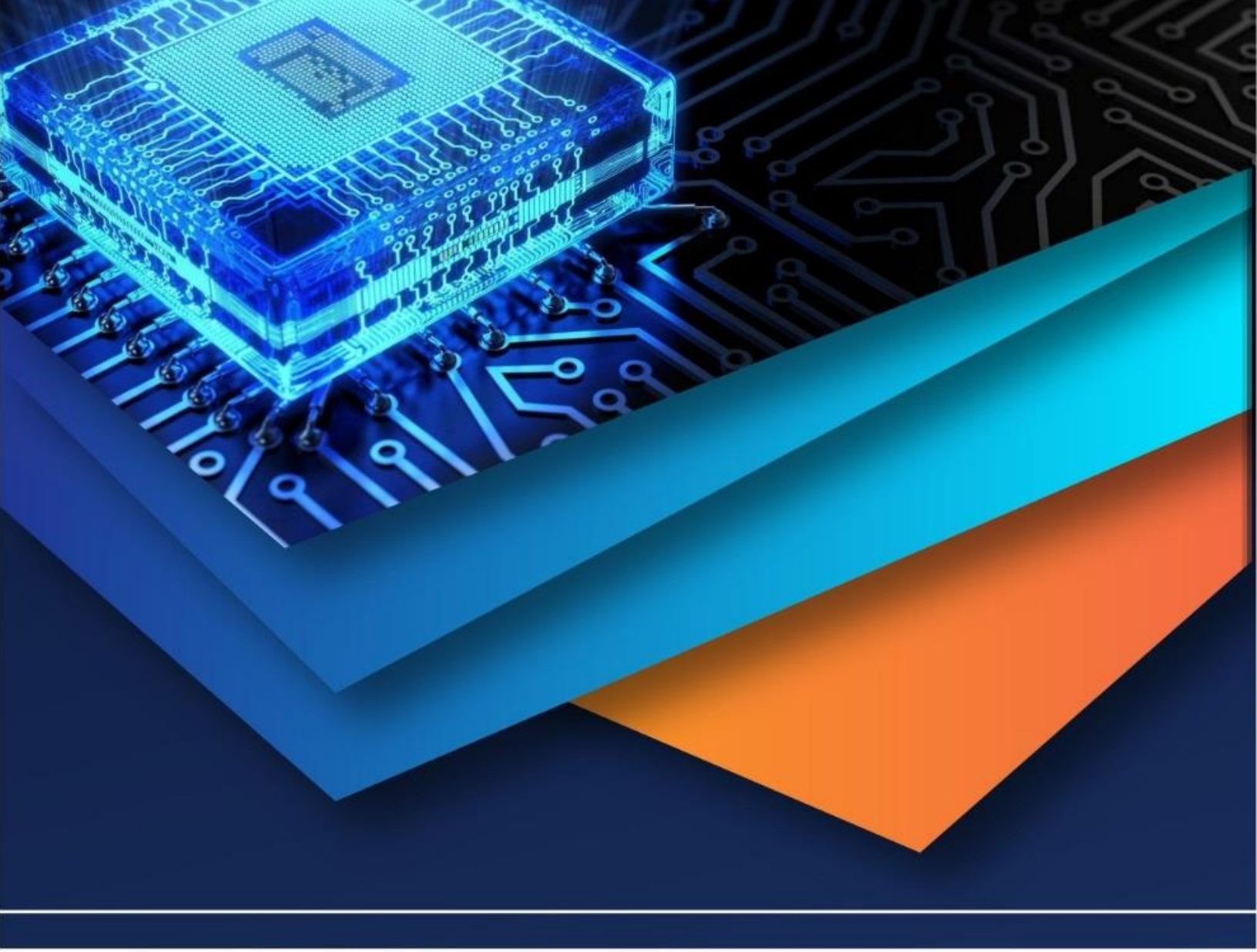
VII. CONCLUSION

In order to lower IT costs and effectively utilize cloud resources, this paper discussed various virtualization techniques, virtualization types, hypervisor techniques, and challenges in cloud computing systems. These techniques included rapid elastic provisioning of virtual machines and elastic application programming models. Additionally, when customers think about security and elastic resource management issues before utilizing the cloud, the virtualization solutions receive widespread acceptance. Future work will focus on creating new frameworks, policies, and methods for maintaining the availability of elastic resources and data, which will improve cloud service performance to the next level. This research paper covered a range of cloud service-related topics that can be used to create a solid framework for efficient elastic resource management in the cloud.

REFERENCES

[1] Mell, P., Grance, T., & Grance, T. (n.d.). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.
[2] Bohar Singh1 , Gursewak Singh2, A Study On Virtualization And Hypervisor In Cloud Computing, Bohar Singh et al, International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 1, January- 2018, pg. 17-22.
[3] Z. Pan, Q. He, W. Jiang, Y. Chen, and Y. Dong, ―Nestcloud: Towards practical nested virtualization,‖ in Proceedings. Int. Cloud and Service Computing (CSC) Conf, 2011, pp. 321–329.
[4] W. Dawoud, I. Takouna, and C. Meinel, Infrastructure as a service security: Challenges and solutions‖, in Proc. Informatics and Systems (INFOS), 2010 The 7th International Conference on, 2010, pp. 1 –8.

[5] A. Whitaker, M. Shaw, S. D. Gribble, ―Denali: Lightweight virtual machines for distributed and networked applications‖, Tech. rep. (Feb. 08 2002).
[6] IBM,―IBM systems virtualization‖, version 2release1,http://publib.boulder.ibmcom/infocenter/eserver/v1r2/topic/eica y/eicay. pdf (2005).
[7] Calheiros RN, Buyya R, De Rose CAF, ―Building an automated and self-configurable emulation testbed for grid applications‖, Software: Practice and Experience, April 2010; Vol. 40(5), Pp. 405–429.
[8] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, ―Xen and the art of virtualization‖, In SOSP '03: Proceedings of the nineteenth ACM symposium on operating systems principles (New York, NY, USA, 2003), ACM Press, pp. 164–177.
[9] Asma ben letaifa, Amed haji, Maha Jebalia, Sami Tabbane, ―State of the Art and Research Challenges of new services architecture technologies: Virtualization, SOA and Cloud Computing‖, International Journal of Grid and Distributed Computing 3(4), December 2010, 69-88.
[10] IBM Virtual Infrastructure Access Service Product. https://www 935.ibm.com/services/au/gts/pdf/end03005usen.pdf.
[11] B. Siddhisena, Lakmal Wruasawithana, Mithila Mendis, ―Next generation muti tenant virtualization cloud computing platform‖, In: Proceedings of 13th International conference on advanced communication technology(ICACT), vol. 12, no.3; 2011. p.405–10.
[12] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009.
[13] Timur Mirzoev, Baijian Yang, "Securing Virtualized Datacenters", International Journal of Engineering Research & Innovation, vol. 2, no. 1, spring 2010.
[14] J. Rutkowska, "Subverting Vista Kernel For Fun and Profit", Aug 2006, Black Hat conference. http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf.
[15] Tim Mather, Subra Kumaraswamy, Shahed Latif, ―Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)‖, O'Reilly Media, Sep.2009;ISBN: 9780596802769 .http://oreilly.com /catalog/97805968027 76
[16] Z. Xiao and Y. Xiao, ―Security and Privacy in Cloud Computing‖, IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY