

Hypervisor and Virtualization in Cloud Computing

Bhavisha Patel¹, Vatsal Joshi² and Dr. Vatsal Shah³

¹⁻²Student, Department of Information Technology, BVM Engineering College
Vallabh Vidyanagar, Gujarat, India

Email: pbhavu15@gmail.com, vatsalnjosshi@gmail.com

³Assistant Professor, Department of Information Technology, BVM Engineering College
Vallabh Vidyanagar, Gujarat, India

Abstract—In today's modern times, hypervisor and virtualization in cloud computing is the most demanding researched topic. In IT industry cloud computing is an emerging field because all are embracing virtualization as a way to cut the expenses and to enhance security. Using hypervisor in virtualization is very significant to achieve system security, flexibility and reliability. In this paper, we discussed and reviewed ten different research paper to get the deeper insights on hypervisor, virtualization and cloud computing.

Index Terms— Cloud computing, Hypervisor, Virtualization.

I. INTRODUCTION

In simple words, cloud computing is a technology that is used for storing and managing data on remote servers through internet. Cloud computing is easy to use because it allows the access of resources like networks, services, storage and servers conveniently anywhere and anytime to user with the pay as per usage service. Virtualization is a central part in cloud computing as provides the potential of running multiple instances on a server. It divides the physical resources, servers into virtual containers which are called virtual machines. In cloud hosting platform, Hypervisor is a form of virtualization software. Hypervisor is a software layer that separates the operating system from physical hardware and can monitor and virtualize the resources of a host machine.

II. LITERATURE REVIEW

A. Ref[1]: (Adesh Kumar, 2020).

This paper examines the research issues in virtualization in cloud computing by studying the characteristics and service models of cloud computing, how virtualization can be useful in different scenarios and then discussing the different concerns that are being faced by hypervisor and virtualization.

With the flexible use of cloud computing technology, the users are able to access its resources from any place via laptops, mobiles, etc. Some of the characteristics of cloud computing that are discussed are-

- Location independent resource pooling: The hardware and software resources are allocated and deallocated to users as per their demands and they had no access to the exact location of resources.
- Elasticity: The cloud has the ability to increase or decrease the computing resources as per the requirement.

- Measured services: There is no upfront cost required to access the resources, the user pays only for the services that they are consuming as per their usage on rental basis.
- On Demand Resource Provisioning: This characteristic allows users to obtain services from cloud directly which saves time, labor and human intervention.
- Broad Network Access: Big enterprises and applications solutions are available over the network through cloud.

The services models of cloud computing are-

- Software as a Service: SaaS resides on top of model and is used by end users.
- Platform as a Service: PaaS is the second layer and is mostly used by programmers to develop and deploy codes in clouds.
- Infrastructure as a Service: IaaS is the third layer that manages the physical resources in cloud.

In general, virtualization is a technology that divides or combines computing resources using different methodologies. Virtual Machine Monitor (VMM) is a virtualization layer which resides above the hardware and below the operating system. Virtualization is useful in many cases like for Sandboxing, Debugging, Software migration, Server consolidation, Testing, Application consolidation, in executing multiple environments, enabling multiple simultaneous OS and many more. Another benefit of virtualization is the scalability that it provides to cloud computing. It provides ability of running multiple instances of an operating system on a single server. There are different types of virtualizations like client virtualization, storage virtualization and server virtualization. The benefits that are gained by virtualization are-

- Productivity: It can be enhanced by using the multiple copies of OS to achieve scaling in an application written for non-scalable OS by avoiding rewriting.
- Performance: The performance of HPC applications can be improved in many ways by virtualization as it provides specialized operating systems that are performance optimized.
- Reliability and Availability: The software or hardware failure affects only one VM because of VM isolation, unless the hypervisor itself suffers the failure.

The Hypervisor is used to isolate the physical hardware from operating system of virtual machines. Due to this if the attacker gets access to host hypervisor, then they are able to access all the virtual machines running on physical machines. Therefore, there are many security concerns like- Resource allocation, virtual machine attacks, migration attacks, etc.

Therefore, virtualization is very important for cloud computing as it brings scalability and also affordable for consumers.

B. Ref[2]: (Obasuyi et al., 2015).

This paper examines the virtualization hypervisors, uses and implementation ways for virtualization, types of hypervisors, types of virtualizations and its advantages. Also, the virtualization security. Due to the growing business needs, the IT resources are being shared over the network via mobiles, laptops, etc. So, the involvement and use of virtualization and hypervisor has also increased to provide security and scalability.

Virtualization is an abstraction layer between hardware and operating system that allows multiple resources to get hold of hardware and software resources of host machine. It provides the power of virtualization to large enterprises by virtual infrastructure. There are many uses and implementation ways like server and application consolidation, virtual hardware, debugging, business continuity, software migration, sandboxing, multiple execution and running multiple simultaneous operating system. Hypervisors are also called Virtual Machine Monitor. Hypervisor allows more than one guest machine to use the physical machine. The two types of hypervisors are –

- Bare metal or Native Hypervisor: This type of hypervisor runs above the host machine so the hardware resources can be accessed directly. It monitors the operating system running on both of the guest machine and also above the hypervisor. Microsoft Hyper-V, VMWare ESX and Xen are the hypervisors of this type.
- Hosted Hypervisor: This is hosted on already installed operating system so the problem occurring in host operating system will influence both the guest operating system and the hypervisor itself. Its examples are VMWare workstation, Oracle VM Virtual Box.

Different types of virtualizations discussed are:

- Para virtualization: The modifications are allowed to be done on guest machine operating system that is working in the virtual environment.
- Full virtualization: The software is allowed to be virtualized by hardware without any modification.

- Partial virtualization: Here, some programs are modified because of all the host machines are not simulated in the virtual environment.
- Application virtualization: Here, the virtualization of applications is done without modifying the host machine.
- Operating System virtualization: The desktop of host machine is moved from physical operating system to virtual environment.
- Nested virtualization: It allows the ability of deploying one virtual machine over another virtual machine by running one or more hypervisor inside another hypervisor.
- Memory virtualization: It shares memory from one or more machines for applications to use either by logically or virtually.

There are several advantages of virtualization like security is achieved because of the isolation of VM. It is reliable because failure of one guest machine doesn't affect the another. It is cost effective and can be easily optimized as per the workload difference. It also provides load balancing and legal applications. In the same physical infrastructure, there are multiple zones available in a VM so this can create the security issues due to which attacker can get full access to the hypervisor environment. Several benefits of security provided by virtualization are-

- Abstraction: The hardware access is restricted by operating system by abstracting the details of hardware which adds security to hypervisor.
- Isolation: The attack on virtual machine doesn't affect the guest machines because the hypervisor creates segments of physical resources
- State restore: This provides data integrity by restoring guest operating system to an earlier time.
- External monitoring: Malicious software outside the VM is detected as virtual machine runs on separate virtual machine.

Therefore, there are several features provided by virtualization that are helpful for various applications with security.

C. Ref[3]: (T. Swathi et al., 2014).

This paper examines the virtualization concerns because virtualization in cloud computing is growing at fast pace in IT world as the resources can be used anywhere at any time with clouds.

Cloud is a computing system which consists a set of inter connected and virtualized computers which gives access to one or more computing resources as per the requirements between service providers and consumers in a parallel and distributed environment. Cloud computing offers computing power, software and storage as a service. Clients, Data Centres and Distributed server are the main components of cloud computing. SaaS, PaaS and IaaS are the three types of cloud services. Clouds also has the limitations like data storage, privacy and security issues. Cloud has three deployment models which are like networking, hardware and software infrastructure, storage provided to the clients. These three models are –

- Public cloud: It is open for general use and is owned by cloud provider. It also provides the feature of multi tenancy. Amazon EC2 is the example of public cloud.
- Private cloud: It is available to a specific consumer and is owned and managed by the organizations as it is arranged under the internal enterprise datacentre of organization. Cloud educational projects in Northern Ireland is the example of private cloud.
- Hybrid cloud: Applying both the features of public and private cloud in a same organization is the hybrid cloud. Scalability, flexibility, cover legacy, cut energy and security can achieved by hybrid cloud. Enterprises hosting e-commerce services is the example of hybrid cloud.

In computing, virtualization means the creation of something virtual like operating system, storage, network devices, hardware or software platform. Cloud is inefficient without virtualization because it adds the feature of scalability to clouds. There are several advantages of virtualization in cloud computing like it easily manages the resources. It abstracts and isolates the resources. It provides security by protecting integrity and also it is cost effective.

Hypervisor is the virtual machine manager which enables multiple operating system runs on a single system without any interference with each other. To monitor the activities of guest virtual machine the advanced protection system is required as hypervisor controls all the guest systems.

Therefore, the strong encrypting techniques are required for secure use of the virtualization in the cloud environment. This can be done by checking client identities, enabling secure migration from private to public cloud. Also, datacentres and devices of clients should be secured by computer policies that are trustworthy.

D. Ref[4]: (Poojara et al., 2017).

This paper examines the performance of different hypervisors using benchmarking tools. In this paper the experiment is carried out on three hypervisors. Xen as native hypervisor, Virtual Box 5.0 and VMWare Workstation 9.0 as hosted hypervisors.

Benchmark can be considered as the evaluation of best practice performance. CPU speed, Memory speed and RAM usage are the performance aspects for benchmarking.

VMWare workstation enables the user to build a virtual machine in windows or operating system as the hosted hypervisor. Virtual Box is a hosted hypervisor that installs on your computer whether it is running on Windows, Mac, Linux or Solaris operating system. The hard disk space and memory are the only limitations of Virtual Box. Xen Hypervisor is an open-source native or bare metal hypervisor. It is used for scheduling of CPU and the partitioning of memory of various virtual machines running on the hardware. Benchmarking gives us the guidance of choosing the appropriate hypervisor from the hypervisors that are available in the market. In the experiment carried out in this paper stress and glances are used as benchmarking tools. Stress is used to create stress on hypervisor and Glances is used to monitor Linux operating system from text interface to analyse the performance. The factors considered for benchmarking the performance in this experiment are-

- CPU: Here the percentage of CPU consumption is analysed by stress for the time it is being consumed to complete task.
- RAM: It measures the percentage of RAM usage and it is stressed by two processes.
- Disk Read and Write Speed: Disk is stressed with process to give the read and write speed of the disk.
- N/W Read and Write Speed: Here, the network transmission and receiving speed is checked.

In this paper, for experiment the stress command is executed and the performance is monitored for 40 seconds of timeline. Here, the final result is obtained after carrying out this experiment 25 times on each hypervisor. The result obtained in this paper from the experiment is that the Xen server gives the best CPU performance. The best RAM performance is given by the VMWare Workstation and the best N/W performance is given by the Virtual Box.

As the performance of the hypervisors can be affected by different factors like the resources and environment. Therefore, the performance of hypervisors may vary according to the circumstances.

E. Ref[5]: (Budhprakash et al., 2016).

This paper examines the hypervisor models and through an experiment they are trying to compare them and find the best hypervisor among KVM, Hyper-V, ESXI and Xen server hypervisor according to their performances. In this paper, the hypervisors are categorized into-

- Para virtualized Hypervisor: This modifies the guest operating system and it is used by Xen hypervisor. Also, Xen server provides good virtual infrastructure.
- Full virtualized Hypervisor: Microsoft Hyper-V and VMWare ESXI 6.0 uses and supports full virtualization. It supports both these servers to provide better performance.
- Hybrid model: This makes use of both the features of para and full virtualization to get the best of them in one. KVM supports the hybrid hypervisor.

In this paper, the experiment is carried out by installing Virtual Machine Windows 12 in all hypervisors. The information performance is measured using SIGAR system and system's workload performance is evaluated using Passmark. CPU, Memory, I/O and Network are taken as measurements for performance evaluation. Also, Cloudstack is used to create private virtual environment. The result they get after this experiment is that among all these four hypervisors ESXI gives better performance but the memory and network performance is good of Hyper-V and KVM.

Therefore, after studying this experiment it is understandable that Hyper-V gives good performance in network and CPU memory whereas Xen server performs better in CPU memory and disk I/O performance. KVM needs improvement in all the areas of measurements. And the ESXI performance turned out to be best among all the hypervisors.

F. Ref[6]: (Samjhana Rayamajhi & Zinnia Sultana, 2014) .

This paper examines the virtualization concept and performance comparison based on its technical features and various benchmarking measurements like file I/O, CPU speed, sequential read-write, memory and cache performance. Through this comparison, guidance is provided to choose the best hypervisors. For their experiment, they researched on VMWare, Virtual Box, KVM and Xen. Xen and KVM are bare metal hypervisors whereas VMWare and Virtual Box are hosted hypervisors. For the setup, Windows 8 Professional is taken as OS, Intel Core i5 430M as Processor, Memory of 4GB Dual Channel DDR3 and Storage of 320GB. Also, 1tb external hard disk is virtualized. Also, three instances of Linux, Ubuntu and two windows 7 operating system are created on the top of each virtualization technology.

Through technical comparison, it is found out that for configuration, editing, migration of virtual machine and updating in virtual box is better and it also supports large range of hard disks whereas VMWare is better in USB and graphics support. Then, KVM is not a better option as compared to Xen in the category of native hypervisors because Xen provides good security. But, KVM is also good in memory page sharing and I/O latency.

Through benchmark comparison, Xen performs better for CPU speed where the CPU overhead performance is checked to find out the dominance time on IRQ servicing routines. Also, Xen is the winner for memory and cache performance as it has good feature of nested page table. Virtual Box is good in sequential read-write performance but KVM and Xen are weak in it. Memory allotment is the one of the most affecting limitation of Virtual Box. So, overall Xen is winner from the point of view of memory and CPU. For read performance VMWare is good whereas for write performance virtual box is good.

Therefore, KVM provides better feature experience and is good fit for deployment but it is not so good for usability as its performance is poor in it. In some areas VMWare and Virtual Box performs better whereas in some Xen is winner. So, there are many limitations of virtualization and multi tenancy in some of the areas. So, it is difficult to figure out which works best for one based on the benchmark comparison because choosing the right hypervisor is based on many factors like the user's needs, their purpose and many more.

G. Ref[7]: (Aaqib Rashid & Amit Chaturvedi, 2019) .

This paper examines how virtualization contributes to cloud computing and also the virtualization technologies. As, cloud computing is used for storing and accessing the data over the internet with its characteristics like resource pooling, broad network access, fast elasticity, measured service and also self-service. Virtualization can be described a technology that isolates the physical resources and uses them as virtual machines. Virtualization provides the benefits of isolating the guest operating system, grouping of all virtual machines in one file and also the hardware independence. There are many advantages of virtualization like it allows rapid deployment of resources, it is cost-effective, it reduces workload and is also efficient for use. Virtualization also has disadvantages like it has still limitations in the area of security risks, scalability and availability issues and also takes time with high cost of implementation.

In cloud computing, virtualization increases the security by providing integrity to cloud components and it is also reliable because it can be scaled up or down as per the requirements and demand. Hypervisor is the abstraction layer between the hardware and operating system that monitors and virtualizes the resources of host machine. The virtualization techniques are-

- Emulation: This technique transforms the role of hardware to a software program and provides flexibility to the guest operating system.
- Full virtualization: Here, the operating system and their hosted software runs on top of the virtual hardware in which the service requests get separated from the physical hardware.
- Para virtualization: Here, the instruction set architecture of host machine is replaced by special hypercalls and it improves the efficiency of communication between guest operating system and hypervisor.

There are several types of virtualizations like-

- Server virtualization: The task of multiple servers is performed by the single server by splitting out the resources of individual server across the multi environment. Also, this type of server is commonly used and it is subdivided into Para virtualization, full virtualization and partial virtualization.
- Client virtualization: Here, the client machines are virtually monitored and updated by system administrator. Hosted or remote virtualization, local or client virtualization and application virtualization are its three types.

- Storage virtualization: Here, the abstraction of logical storage from physical storage is created. Network Attached Storage, Direct Attached Storage and Storage Area Network are three kinds of storage used in virtualization. Also, Block and File are the two types of storage virtualization.
- Network virtualization: It provides improved network productivity and efficiency by managing and monitoring the computer network from the console of single software-based administrator. Internal and External are two categories of network virtualization.
- Memory virtualization: Distributed and shared memory is provided by decoupling the memory from the server.
- Software virtualization: The one or more virtual environments are created and run on the complete computer system. Operating system, application virtualization and server virtualization are three types of software virtualization.
- Desktop virtualization: The flexibility of working from any location along with security is provided in this type of virtualization.

Therefore, virtualization brings many benefits to cloud computing like security, scalability, flexibility, cost-effectiveness and also productivity.

H. Ref[8]: (Ramakrishna Subbareddy & Dr. B. Firdaus Begam, 2021).*

This paper examines the understanding of virtualization and its types, hypervisor and its types, and also safety management of hypervisor.

Virtualization creates a layer between the hardware and software as an abstraction. There are several types of virtualization like full virtualization, hybrid virtualization, para virtualization, partial virtualization, OS-level virtualization and hardware assisted virtualization. Here, hypervisor is responsible for all the files that works on virtual hardware. Hypervisor is also known as Virtual Machine Monitor and it enables multiple virtual machines and operating system to run on the single physical server. Bare Metal Hypervisor and Hosted Hypervisor are two types of hypervisors:

- Bare Metal Hypervisor: This type of hypervisor is directly installed in a physical server and mainly it is used on servers. Also, the access is provided to the hardware components. Xen Server, Esxi, KVM and Hyper-V are examples of bare metal hypervisor. Full virtualization needs no modification to the core OS whereas the para virtualization needs modification to work but it is good in performance tuning. Xen server and Esxi supports both full and para virtualization whereas KVM and Hyper-V supports only full virtualization. Better security with direct access to hardware are the advantages of bare metal hypervisor. Cost and the requirement of specific hardware are its disadvantages.
- Hosted Hypervisor: This type of hypervisor runs between the hardware and the virtual machines and also other virtual machines can run on existing virtual machine because this type of hypervisor is placed above the operating system. Also, separate installation of software is not needed to build the virtual environment. Virtual PC and VMWare workstation supports both full and para virtualization whereas KVM and Virtual Box supports only full virtualization. Multiple OS capability with hardware is accessed by host OS are its advantages. Requirement of host OS and security risks are its disadvantages.

Network communication is very important for interaction between hypervisor and user. For hypervisor security the understanding of APIs and basic knowledge on visual equipment is very important. Authentication, Authorization and network communication are the three stages for safety management of hypervisor.

Therefore, virtualization is vastly used by big enterprises to optimize the IT costs. Both the hypervisors have their own advantages and disadvantages. And some performance measures are also taken to improve the security of hypervisor and also of virtualized systems.

I. Ref[9]: (Durairaj. M & Kannan.P, 2014).

This paper examines how virtualization is helping cloud computing environment to improve the elasticity of resources. Also, providing detailed insights on the virtualization techniques and the challenges in the acceptance of virtualization

Virtualization provides encapsulation of virtual machines creating abstract layer of system resources. Virtualization is diverting the perspective of using IT resources from physical to logical. Server virtualization, client virtualization and storage virtualization are its types. Several virtualization techniques are:

- Emulation: It provides flexibility by converting the role of computer hardware to software program.

- Hypervisor: It is layer between hardware and operating system to monitor and virtualize the resources of host machine.
- Para virtualization: Here, the instruction set of architecture is substituted by the special hyper calls and accessing the resources is easier than full virtualization.
- Full virtualization: Here, the operating system directly accesses the controls of hardware without the knowledge of virtualized environment and modifications in it.

There are many factors affecting in the development and acceptance of cloud computing and virtualization because of many management aspects. They are-

- Data leakage: There is high risk of data leakage when the data is stored cloud system because the attacker can access it at hypervisor level.
- Virtualization security threats: Virtual machine, hypervisor, virtual infrastructure and virtual network threat are the classification of virtualization security threats.
- Data remanence issue: Here, the users are not given the permission to securely delete the data from the physical device of cloud provider. So, there is a possibility that these data can be recovered by malicious users.
- Privacy: The concerns that are faced by cloud users are the storage issues, assurance of destruction time policy of cloud provider, data breaches and also the regular auditing and monitoring policies.
- Elastic resource management: Resource allocation, provisioning, mapping and adaptation can be achieved by the effective implementation of elastic resource management.

There are various obstacles in development and acceptance of virtualization and cloud computing but with the different techniques and effective implementation of the elastic resource management the cloud services security issues can be improved.

J. Ref[10]: (Joshi et al., 2015).

This paper examines the hypervisor forensics to analyse the security threats and the attacks on Hypervisor system. As the hypervisor in the virtualization is at upfront of being attacked by attackers. So, there is need to proposed and understand the models for security and also to understand the challenges being faced in implementing these models and also to create awareness in the area of hypervisor forensics.

Hypervisor is the application layer that acts as an interface between the physical host machine and the guest operating system. The methodology of carrying out the post investigation of attack to find out the evidence and source of attack is called hypervisor forensics. Also, there are many challenges and gaps in the research field of hypervisor forensics. The way of taking full control of hypervisor from virtual machines is called virtual escaping. There are many strengths of Hypervisor based systems like as the hypervisor is on the upper layer, so security is provided at this level to get access. It prevents the attacker to approach the shared physical hardware as it acts like a firewall and the hypervisor also has the ability of monitoring network in cloud environment. Also, there are weaknesses like security threats from wrapping attacks, single point failure due to flooding attack, D-dos attack. The possible attacks on hypervisor system are-

- Wrapping Attack: This type of attacks duplicates the authentic user during login phase to affect the Simple Access Object Protocol messages which are being exchanged during the setup of web browser and server. This is a threat to virtual environment.
- Data stealing: In this the data is steal from authorized user without leaving any trace of data and this is can be prevented by applying some policies like RAID.
- D-dos Attack: This type of attacks damages the computer system resources by flooding the IP packets at specific networks. So, if hypervisor is not able to provide sufficient VMs than the risk of D-dos attack increases.
- Client to Client Attacks: In this type of attack the attacker accesses the administrative authorization and put malicious content from one virtual machine which creates a disrupt in other machines.
- Vulnerable interfaces and API's: The data integrity, confidentiality can be at high risk at hypervisor level due to vulnerable API's and interfaces.

The methodology of analysing and collecting evidences for crimes scenes is called forensics. The different types of forensics discussed are-

- Digital forensics: Here the investigation is carried out by collecting, identifying, validating and analysing the digital data logs.
- Network forensics: Here, the data is analysed from network traffic by firewalls, capturing packets and also through devices like routers.

- Cloud forensics: Here, for investigation purpose the information is collected from clouds.
- Hypervisor forensics: The data that is passing from guest OS to the hypervisor layer before physical devices can be used as log evidence for investigation in hypervisor forensics.

The problems that are being faced for investigation in hypervisor forensics are-

- Identification: In distributed cloud environment, getting evidences for identification of sources is a tedious task. So, for forensic investigation at hypervisor level data loss in volatile storage is a challenge in virtual environment.
- Collection: Collecting log evidences for investigation from virtual environment is a difficult task because cloud computing is in distributed environment.
- Preservation: Preserving the evidences of the relatives and trustworthy one is another issue that forensic investigation is facing.
- Analysis: Due to the limited log evidence processing, the analysis becomes difficult.
- Reporting: Reporting is an issue in virtual environment because the availability of cloud resources, crime location is difficult to investigate.

Therefore, there are many possible attacks in the virtual environment and there are many issues and challenges faced by the investigators. But all these problems can be solved with the proper research and doing further studies in the area of hypervisor forensics.

III. CONCLUSIONS

In this paper, we write a review on ten different research papers. We discussed the cloud computing characteristics, its cloud services. Then the virtualization types, its techniques, the challenges it is facing, advantages and disadvantages. Also, discussed about hypervisor in detail, its types and the comparison among different hypervisor to choose the best through benchmarking, different attacks on hypervisor systems and how hypervisor forensics is emerging to find the better techniques in the area of internet crime for investigation. Therefore, cloud computing cannot stand alone without virtualization as it bringing many solutions and benefits to the IT industry. Also, some techniques and applications with the research can solve the problems that are in the limitations of virtualization and hypervisor in cloud computing.

REFERENCES

- [1] Adesh Kumar (2020, January 4), "Research Issues in Virtualization in Cloud Computing", *International Journal of New Innovations in Engineering and Technology*, vol. 12, pp. 150–159.
<http://www.ijniet.org/wp-content/uploads/2020/10/24.pdf>
- [2] Obasuyi, G.C. and Sari, A. (2015), "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment.", *Int. J. Communications, Network and System Sciences*, vol. 8, pp. 260–273.
<http://dx.doi.org/10.4236/ijcns.2015.87026>
- [3] T. Swathi, K. Srikanth and S. Raghunath Reddy (2014, May 5), "Virtualization in cloud computing", *International Journal of Computer Science and Mobile Computing*, vol. 3, pp. 540–546.
<https://www.ijcsmc.com/docs/papers/May2014/V3I5201499a.pdf>
- [4] Shivananda R. Poojara*, N. V. Dharwadkar and Vishal Ghule (2017, November), "Performance Benchmarking of Hypervisors - A Case Study", *Indian Journal of Science and Technology*, vol. 10(44).
https://indjst.org/download-article.php?Article_Unique_Id=INDJST3966&Full_Text_Pdf_Download=True
- [5] Budhprakash, Dr. Anupam Bhatia and Dr. Gurjeetsingh Bhattal (2016, December 12), "A comparative study of Various Hypervisors Performance", *International Journal of Scientific & Engineering Research*, vol. 7, pp. 65–71.
<https://www.ijser.org/researchpaper/A-comparative-study-of-Various-Hypervisors-Performance.pdf>
- [6] Samjhana Rayamajhi and Zinnia Sultana (2014, September 9), "Comparative Performance Analysis of the Virtualization Technologies in Cloud Computing", *International Journal of Engineering Research & Technology (IJERT)*, vol. 3, pp. 1269–1272.
<https://www.ijert.org/research/comparative-performance-analysis-of-the-virtualization-technologies-in-cloud-computing-IJERTV3IS090667.pdf>
- [7] Aaqib Rashid and Amit Chaturvedi (2019, April 4), "Virtualization and its Role in Cloud Computing Environment", *International Journal of Computer Sciences and Engineering*, vol. 7, pp. 1131–1136.
https://www.researchgate.net/publication/333642946_Virtualization_and_its_Role_in_Cloud_Computing_Environment
- [8] Ramakrishna Subbareddy* and Dr. B. Firdaus Begam (2021, February 2), "A Study on hypervisor virtualization in cloud computing", *International Journal of Scientific & Engineering Research*, vol. 12, pp. 264–268.
<https://www.ijser.org/researchpaper/A-Study-on-hypervisor-virtualization-in-cloud-computing.pdf>
- [9] Durairaj. M and Kannan.P (2014, November 11), "A Study On Virtualization Techniques And Challenges In Cloud Computing", *International Journal of Scientific & Technology Research*, vol. 3, pp. 147–151.

<https://www.ijstr.org/final-print/nov2014/A-Study-On-Virtualization-Techniques-And-Challenges-In-Cloud-Computing.pdf>

- [10] Lalit Mohan Joshi, Mukesh Kumar and Rajendra Bharti (2015, June), “Understanding Threats in Hypervisor, its Forensics Mechanism and its Research Challenges”, *International Journal of Computer Applications*, vol. 119 (1).
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.4606&rep=rep1&type=pdf>