International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

The Impact of Hypervisors towards Cloud Computing

Chhaya Porwal[1*], Chandra Prakash Singar[2], Puja Gupta[2]

[1]Data Specialist, IBM India Pvt Ltd
[2]Assistant Professor, MANIT, Bhopal, M.P. India
[2]Assistant Professor, Shri G.S. Institute of Technology & Science, Indore, M.P. India

Abstract

Hypervisors, fundamental in cloud computing, facilitate the operation of multiple virtual machines on a single physical hardware system. This technology enables efficient resource utilization, cost savings, and improved scalability in cloud environments. As the backbone of virtualization, hypervisors have a pivotal role in diverse cloud services and deployments. This abstract explores the significance of hypervisors in cloud computing, emphasizing their role in managing multiple virtual environments, optimizing hardware resources, and ensuring security and isolation among virtual machines. In this context, we delve into key hypervisor types, such as Type 1 (bare-metal) and Type 2 (hosted), discussing their functionalities, performance, and compatibility. Moreover, we examine prominent hypervisor solutions like VMware vSphere, Microsoft Hyper-V, and open- source options such as KVM and Xen, considering their features, performance, and support for various operating systems. Understanding hypervisors' importance and their role in cloud infrastructure is essential for businesses and users seeking the optimal virtualization solution for their specific requirements. Keywords: Hypervisor, Virtualization, Cloud Computing, VMware vSphere, Microsoft Hyper-V, KVM, Xen. Understanding the nuances of hypervisors in cloud computing is crucial for businesses and organizations seeking the ideal balance between performance, security, and cost- efficiency. By abstracting physical hardware, they enable the consolidation of multiple VMs onto a single server, optimizing resource allocation and enhancing overall system.

Keywords: Hypervisor, Virtualization, Cloud Computing, VMware vSphere, Type 1 Hypervisor, Type 2 Hypervisor

1. INTRODUCTION:

In the realm of cloud computing, where the optimization of resources and the efficient allocation of computing power are paramount, the role of hypervisors stands as a linchpin. Hypervisors[1], the underlying software that creates and manages virtual machines, serve as the cornerstone of modern cloud infrastructures. These sophisticated tools enable the abstraction of physical hardware, allowing multiple virtual environments to operate on a single physical server. As the technological backbone of virtualization, hypervisors play a pivotal role in driving resource efficiency, scalability, and security within cloud environments.

The concept of virtualization[2], facilitated by hypervisors, has transformed the landscape of computing by abstracting hardware resources from the underlying physical infrastructure. This abstraction empowers the seamless operation of multiple independent virtual machines, each running its own operating systems and applications. By encapsulating these virtual environments, hypervisors enable enhanced workload isolation, providing a secure and scalable ecosystem for diverse applications, services, and users in the cloud. Understanding the diverse types of hypervisors, their functionalities, and their impact on cloud infrastructure is essential in comprehending the intricacies of modern computing paradigms and making informed decisions in deploying scalable and secure cloud solutions. This introduction aims to illuminate the fundamental significance of hypervisors in the context of cloud computing, delving into their role in managing virtual infrastructures, optimizing hardware resources, and ensuring robust security measures for varied applications.

- Introduce the concept of hypervisors as foundational software that enables the creation and management of virtual machines on physical hardware.
- Highlight the working of hypervisors in cloud computing.
- Briefly touch the concept of Type 1 (bare- metal) and Type 2 (hosted) hypervisors.
- Discuss the security structure within a virtual environment, highlighting the role of a hypervisor.
- Features of hypervisor in relation to security.

2. LITERATURE REVIEW

Hypervisors, pivotal in the realm of cloud computing[1], act as the linchpin technology enabling the creation and management of multiple virtual machines on a single physical server. As noted by various scholars, their fundamental role in abstracting hardware resources from the underlying infrastructure is key to optimizing resource utilization and facilitating the consolidation of diverse workloads in cloud environments. These virtualization tools play an integral role in enhancing scalability, flexibility, and the overall efficiency of cloud infrastructures, serving as a bridge between physical hardware and virtual environments.Academic discourse[2] widely differentiates between Type 1 and Type 2 hypervisors, showcasing their distinct architectures and functionalities. Type 1 hypervisors, operating directly on the bare-metal hardware, exhibit superior performance and efficiency due to their direct interface with the underlying hardware, while Type 2 hypervisors, leveraging a host operating system, offer increased user-friendliness but slightly reduced performance. Comparative studies often discuss their trade-offs, providing insights into their suitability for various cloud setups and workloads.Emphasizes the crucial role of hypervisors[3] in ensuring security and isolation among different virtual machines. Scholars underscore the security mechanisms and measures implemented by hypervisors to maintain robust isolation, prevent cross-VM interference[4], and protect against vulnerabilities, thereby safeguarding sensitive data and applications running in the cloud. Examines the integration & compatibility of hypervisors in intricate cloud systems. Researchers delve into how hypervisors contribute to the orchestration of resources, management of diverse workloads, and their interoperability with various cloud services and applications, emphasizing their integral role in orchestrating a seamless cloud environment.

Academic analyses dive into the performance metrics and benchmarks used to evaluate hypervisors. These studies focus on throughput, latency, CPU usage, and memory overhead, providing a comparative evaluation of various hypervisor solutions. Benchmarking plays a critical role in assisting

cloud architects and administrators in selecting the most performance-optimized hypervisor for their intended cloud infrastructure.Research [5-7] in earlier studies highlighted the pivotal role of hypervisors in ensuring compliance with industry regulations in sensitive sectors. These studies emphasized the importance of secure [8-9] hypervisor designs in facilitating adherence to regulatory frameworks in industries requiring stringent data security and compliance measures.

3. CONCEPT OF HYPERVISOR

A hypervisor, often referred to as a virtual machine manager (VMM)[10], is a critical software component in the realm of virtualization technology. It serves as the intermediary layer between the physical hardware of a computing device (such as a server, desktop, or mainframe) and the virtual machines (VMs)[11] running on that hardware. Its primary purpose is to create, manage, and allocate the underlying physical resources of the host system among multiple VMs.

This pivotal software layer abstracts the physical resources[12], which include the central processing unit (CPU), memory, storage, and network, and presents them to each VM as if they were dedicated resources. It allows for the division and isolation of these resources[13] to ensure that each VM operates independently and securely. Through this abstraction, the hypervisor enables multiple operating systems (and their associated applications) to run on a single physical machine simultaneously. The hypervisor's functionality[14-15] includes resource allocation, management, and optimization. It ensures fair and efficient distribution of resources among VMs based on their needs, dynamically adjusting resource allocations as demanded. Additionally, it establishes boundaries between VMs, preventing interference or unauthorized access[16] between them, thus enhancing security and isolation.

Furthermore, some hypervisors support advanced features[17] such as live migration, enabling seamless movement of VMs from one physical host to another without interrupting service, ensuring high availability and efficient resource utilization. Hypervisors also facilitate the creation of snapshots or clones of VMs, allowing for backup, testing, and replication of VM instances.

In essence, a hypervisor is the linchpin of virtualization, facilitating the creation and management of multiple virtual environments on a single physical machine, delivering benefits such as increased flexibility, scalability, resource optimization, and cost efficiency in IT infrastructures.

3. WORKING OF HYPERVISOR

The hypervisor operates as a crucial layer in virtualization technology, mediating between the physical hardware of a computing device and the multiple virtual machines (VMs) running on it. Its primary function involves abstracting the host machine's physical resources, such as CPU, memory, storage, and network, to create an illusion of dedicated resources for each VM. By doing so, it enables multiple operating systems[18] and their associated applications to run concurrently on a single physical system.

Resource allocation and management are central to the hypervisor's operation. It dynamically assigns and manages these shared resources among VMs based on their needs, ensuring optimal performance across the virtual environment. Furthermore, the hypervisor ensures strict isolation between VMs, preventing interference or unauthorized access, thereby enhancing security and stability. The operational mode of the hypervisor differs between Type 1 and Type 2 hypervisors[19]. Type 1 hypervisors, running directly on the hardware without an underlying OS, have direct access to the hardware resources, managing resource allocation and communication between hardware and VMs.

Conversely, Type 2 hypervisors, hosted on an existing operating system, intercept hardware commands from the VMs, translating and directing these commands to the physical hardware. In addition to resource management, the hypervisor may support advanced features like live migration, enabling the seamless movement of VMs between physical hosts without service interruption. It also allows for the creation of snapshots or clones of VMs for backup, testing, and replication purposes.

Ultimately, the hypervisor serves as the linchpin of virtualization, enabling the creation and management of multiple VMs on a single physical machine. Its operations encompass resource abstraction, allocation, isolation, and support for advanced functionalities, leading to enhanced flexibility, efficiency, and scalability[20] within IT infrastructures. in optimizing resource utilization, ensuring security, and orchestrating complex cloud infrastructures. Furthermore, it identifies potential areas for future research, emphasizing the need for enhanced security measures, performance optimizations, and adaptability to emerging technological advancements for an ever-evolving cloud ecosystem.

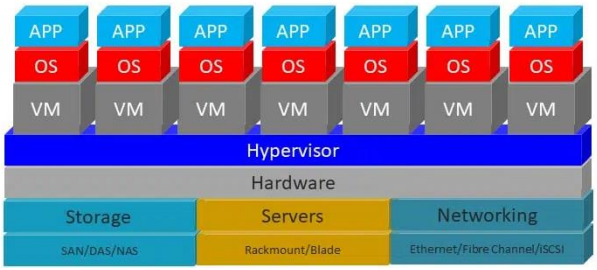

Figure 1: working of hypervisor

4. HYPERVISOR AND VIRTUALISATION

A hypervisor is a type of hardware or software that builds and maintains virtual machines (VMs). It is often referred to as a virtual machine monitor (VMM). Each virtual machine[21] is referred to as a guest machine, while the host machine is the computer on which a hypervisor is installed. The guest OS can run on a virtualized[5] platform that the hypervisor provides. This configuration makes it possible for several instances of Linux, Windows, and macOS to share virtualized hardware resources on a single physical x86 computer.

5.1 Types of hypervisor

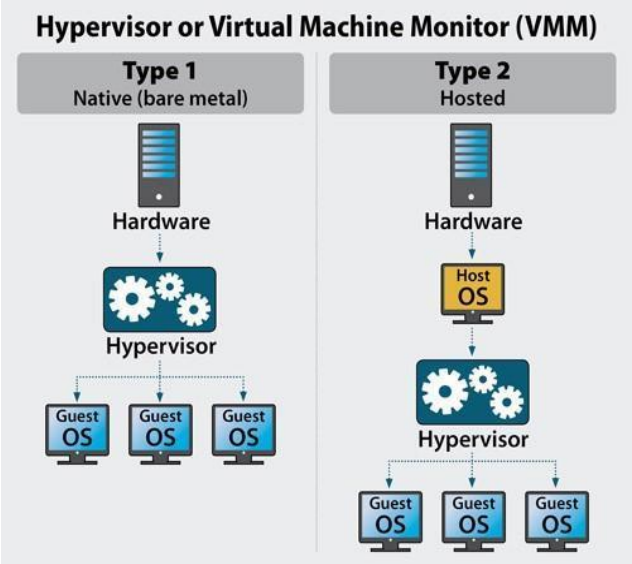

Figure 2: Types of Hypervisor

4.1.1.BareMetal Hypervisor (Type 1):

It is also referred to as "bare metal" or "native hypervisor" since, as Fig. 2 illustrates, it operates directly on top of the underlying hardware. Since there is no operating system running underneath it, in this instance, VMM is a tiny piece of code[23] whose job it is to schedule and assign system resources to virtual machines .Type 1 VMM examples include Xen and VMware ESX. In this instance, the guest OS accesses the underlying hardware directly due to device drivers provided by the VMM [3] Type 1 hypervisors are designed to operate directly on the physical hardware of a host system, bypassing the need for an underlying operating system. This direct approach grants them unparalleled control over system resources and enhances their efficiency and performance. They serve as a virtualization layer between the hardware and virtual machines.

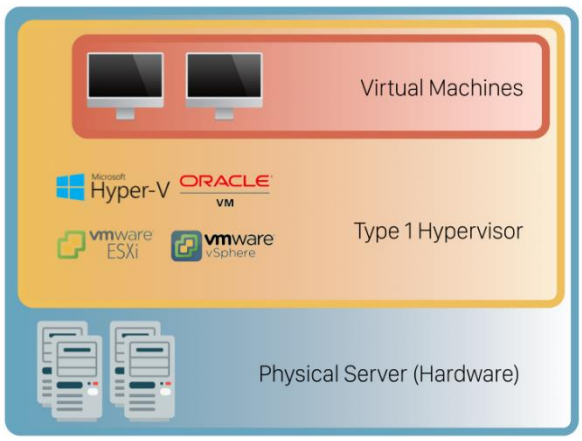

Figure 3: Type 1 Hypervisor

Installation and Operation:

- Installed directly on the bare metal of the host server, independent of an operating system.
- They facilitate virtual machine management and resource allocation directly from the hardware.

Performance and Robustness:

- Boasting high performance, Type 1 hypervisors are well-suited for enterprise-level[24] virtualization in data centers.
- Due to their direct access to hardware, they generally exhibit lower latency and overhead.

Examples of Type 1 Hypervisors:

- *VMware vSphere/ESXi:* One of the most widely used hypervisors in enterprise environments, known for its stability and advanced features.
- *Microsoft Hyper-V (in a bare-metal deployment):* Offers a comprehensive set of tools[25] and integrations for Windows-based environments.

Xen: Renowned for its open-source nature and its ability to manage multiple operating systems on a single host.

Advantages of Bare-Metal Hypervisors (Type1):

- Enhanced security
- Higher density hardware
- Direct access to HW

Disadvantages of Bare-Metal Hypervisors (Type1):

- Need of specific HW component
- Stringent HW requirement
- Expensive

4.1.2.Hosted Hypervisor (Type 2)

The hypervisor, which operates as an application in a regular operating system known as the host operating system, is also referred to as hosted[25] VMM. The host operating system handles Type II VMM as if it were any other process; it has no knowledge of it. Usually, it handles I/O on the guest OS's behalf. The host OS intercepts the I/O request made by the guest OS and forwards it to the device driver responsible for executing the I/O[20-21]. Through the host OS, the completed I/O request is once more routed back to the guest OS [6].

Type 2 hypervisors, in contrast, function as software applications installed on top of a pre-existing operating system. They leverage[33]the host operating system's resources to manage virtual machines, providing a more user-friendly interface for personal or smaller-scale use cases.

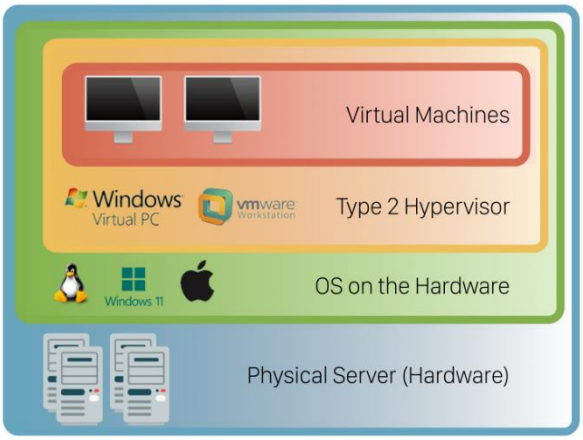

Figure 4: Type 2 Hypervisor

Installation and Operation:

- Installed as an application within an existing operating system, requiring a host environment to function.
- Provides an easier setup and management[26] interface for individual users or smaller deployments.

Ease of Use and Flexibility:

- Ideal for personal computing and testing environments due to their simplicity and user- friendly setup.
- Offers the ability to run multiple operating systems on a single physical machine, enhancing versatility[23].

Examples of Type 2 Hypervisors:

- *VMware Workstation:* Widely used for testing, development, and demonstration purposes, providing an intuitive user interface.
- *Oracle VirtualBox:* Known for its broad compatibility and support for various guest operating systems.
- *Parallels Desktop:* Popular among Mac users for running Windows[26] and other operating systems on macOS.

Advantages of Hosted Hypervisors (Type 2):

- Hardware access is controlled by host OS
- Accessibility ease
- Multiple operating systems compatible

Disadvantages of Hosted Hypervisors (Type 2):

- Reduced security
- Low VM density •Required host OS

Both types of hypervisors have their distinct advantages and applications, catering to different user requirements and scenarios. Type 1 hypervisors excel in high-performance[24], mission-critical environments, while Type 2 hypervisors offer user-friendliness and versatility for personal and smaller-scale usage. Understanding these differences enables users to choose the most suitable hyperviso[25]r for their specific needs.

5. HYPERVISOR SECURITY

Every virtual machine that is installed in the virtual environment has a security zone of its own that is isolated from the security zones of other virtual machines. An abstraction layer called a hypervisor divides the host computer from the guest computers [25]. With its own security zone, a hypervisor serves as the centralized controlling agent for all virtual machines. Within the same physical environment and security zone, all of the virtual environment's security zones were located [26]. Prior to delving into the security concerns surrounding hypervisor security, it is imperative that we gain an understanding of the different CPU privilege modes. Every processor has three privilege levels [27]. These are displayed in Figure 3.

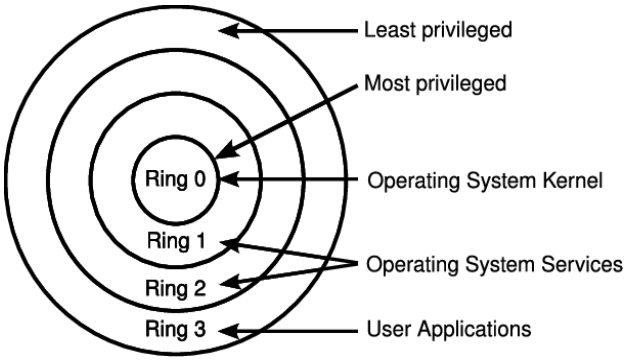

Figure 5: Privilege Level Architecture

Within the protection rings, Ring 0 is the most privileged and innermost level. Kernal level is another name for this level. At this point, any software or application has complete control over the host hardware. Comparatively speaking, ring 0 enjoys greater privileges than rings 1 and 2. Operating System services are connected to these two rings. Ring 3 is the outermost, and all application programs operate on this layer. The guest operating system operates in a less privilege mode than the hypervisor, while the hypervisor operates in the highest privilege level, kernel mode. Figure 4 displays the architecture of the hypervisor along with its privilege level. Ring 3 is where the user application[24] runs, and it has no authority over the hardware resources. The guest operating system can access hardware resources that are managed by the hypervisor[28]. Since the hypervisor runs on the physical hardware's top layer. Because physical resources can only be accessed via the hypervisor, the hypervisor is essential to the cloud environment's security. It also serves as a firewall, preventing physical resources from being shared without authorization. The host operating system[25], the guest operating system, and the physical hardware are all isolated by a hypervisor[28, 29].

Hypervisor keeps an eye on the guest operating system in case an attacker manages to get past the security measures. It functions as a manager between the physical hardware and the guest operating system. The operating system of a guest machine (VM) accesses [26]the physical machine components via the hypervisor [30].

A hypervisor is comparable to thousands of lines of code. to reduce the Hypervisor's vulnerability and avoid security issues. The minimal amount of hypervisor code is desirable. In a virtual environment, an attack typically has three outcomes[31]. In the first example, the compromised machine is the guest machine; in the second, it affects multiple virtual machines; and in the third, it affects the host machine or hypervisor. In the first two cases, the configuration[28-30] can be changed back to the previous, well-known state; however, in the third case, the attackers fully control the hardware. A study on the security[33] of virtual machines (VMs) found that, as a result of conventional security measures being disregarded, between 60 and 65 percent of virtual machines in production[34] are less secure than physical machines.

A hypervisor is comparable to thousands of lines of code. to reduce the Hypervisor's vulnerability and avoid security issues. The minimal amount of hypervisor code is desirable. In a virtualized environment, an attack typically has three outcomes.

CONCLUSION

In the contemporary landscape, virtualization has emerged as an increasingly significant asset, especially within major corporate enterprises striving for cost efficiency and optimal utilization of cloud computing resources. This paper has underscored the prominence of virtualization in cloud computing and has delved into the various types of hypervisors utilized in virtualized environments. The exploration of bare-metal and hosted types of hypervisors has illuminated their respective advantages and drawbacks. While bare-metal hypervisors offer high performance and direct hardware access, hosted hypervisors provide ease of use and compatibility with various systems. The distinct characteristics of each type underscore the need for a nuanced approach in their implementation, based on specific system requirements and preferences.

For the continued enhancement of these virtualized systems, the paper highlights the imperative need for a multifaceted approach encompassing performance optimization, modelling, and simulation. Moreover, the application of robust security measures stands as a critical aspect essential to fortifying these virtualized environments against potential vulnerabilities and emerging threats. As organizations increasingly rely on cloud computing resources and virtualization to streamline operations and optimize costs, ongoing efforts toward improving these systems through advanced performance measures and stringent security protocols remain imperative for sustaining their efficiency and reliability.

REFERENCES

[1] Perez-Botero, D., Szefer, J. and Lee, R.B., 2013, May. Characterizing hypervisor vulnerabilities in cloud computing servers. In Proceedings of the 2013 international workshop on Security in cloud computing (pp. 3-10)

[2] Ramos, J.C.C.D.S., 2009. Security challenges with virtualization (Doctoral dissertation).

[3] P, Galvin B. VMware vSphere Vs. Microsoft Hyper-V: A Technical Analysis. [White Paper] s.l. : CTI Strategy, 2009.

[4] Chen, L., Zhang, J., Cai, L., Li, R., He, T. and Meng, T., 2015. MTAD: a multitarget heuristic algorithm for virtual machine placement. International Journal of Distributed Sensor Networks, 11(10), p.679170.

[5] Gupta, P. and Kulkarni, N., 2013. An introduction of soft computing approach over hard computing. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3(1), pp.254-258.

[6] Huang, J., Wu, K. and Moh, M., 2014, July. Dynamic virtual machine migration algorithms using enhanced energy consumption model for green cloud data centers. In 2014 International Conference on High Performance Computing & Simulation (HPCS) (pp. 902-910). IEEE.

[7] T. Gardinkel.M.Rosenblum,"When Virtual is Harder than Real: Security Challenges in virtual Machine Based Computing Environments,"USENIX Association, 2005.http://www.stanford.edu/talg/papers/HOTOS05/virtualha rder-hotos05.pdf

[8] N.Arya,M.Gidwani and S.K. Gupta," Hypervisor security A makorconcern",International Journal of Infromation and Computation Technology,vol.3, no.6.pp533-538,2013.

[9] M.Ali,S.U.Kan and A.V. Vasilakos,"Security in cloud computing :opportunities and challenges",Information Science,vol.305,pp.357-383,2015.

[10] S.Jin,J.Seol,J.Huh and S.maeng,"Hardware-assisted secure resource accounting under a vulnerable Hypervisor", ACM

[11] Esfandiarpoor S, Pahlavan A, Goudarzi M (2015) Structure-aware online virtual machine consolidation for datacenter energy improvement in cloud computing. ComputElectrEng 42:74–89 (2015).

[12] Dong, J., Jin, X., Wang, H., Li, Y., Zhang, P. and Cheng, S., 2013, May. Energy-saving virtual machine placement in cloud data centers. In 2013 13th IEEE/ACM international symposium on cluster, cloud, and grid computing (pp. 618-624). IEEE.

[13] Choubey, R., Dubey, R. and Bhattacharjee, J., 2011. A survey on cloud computing security, challenges and threats. International Journal on Computer Science and Engineering (IJCSE), 3(3), pp.1227-1231.

[14] A.Ukil,D.Jana,andA.De.Sarkar, " A Security Frwamework in Cloud Computing , "International Journal of Network Security and its Application,vol.5,no.5,pp.11- 24,2013.

[15]]A.Cleeff,W,pieters and R.Wieringa, " Security implications of Virtualization: A literature study". In proceddings of the 12 th IEEE International Conference on Computional Science and engineering (cse09),vol.3,pp.201,2015.

[16] S.k. Majhi and S.K. dhal, "A study on security vulnerability on cloud platforms",inprocedding of rtheIst International confrence on Information security and Privacy 2015.

[17] Lee, K., 2012. Security threats in cloud computing environments. International journal of security and its applications, 6(4), pp.25-32.

[18] L. Turnbull and J. Shropshire, "Breakpoints: An analysis of potential hypervisor attack vectors," in Proceedings of the IEEE SoutheastCon 2013: Moving America into the Future, 2013.

[19] Lopez-Pires, F. and Baran, B., 2015. Virtual machine placement literature review. arXiv preprint arXiv:1506.01509.

[20] Ruan X, Chen H (2015) Performance-to-power ratio aware virtual machine (VM) allocation in energy-efficient clouds. In: IEEE ınternational conference on cluster computing, pp 264–273.
[21] S. Manavi and S. Mohammadalian, "Secure model for virtualization layer in cloud infrastructure," International Journal of Cybersecurity and Digital Forensics, vol. 1, no. 1, pp. 32–40, 2012.
[22] L. Almutair and H. Zaghloul, in Proceedings of the The Third International Conference on Digital Information Processing and Communications (ICDIPC '13), pp. 676–686, UAE, 2013.
[23] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
[24] Kamesh and N. SakthiPriya, "Security enhancement of authen- ticated RFID generation," International Journal of Applied Engineering Research, vol. 9, no. 22, pp. 5968–5974, 2014.
[25] O. Harfoushi, B. Alfawwaz, N. a. Ghatasheh et al., "Data security issues and challenges in cloud computing: A conceptual analysis and review," Communications and Network, vol. 6, no. 1, pp. 15– 21, 2014.
[26] N. Arya, M. Gidwani, and S. K. Gupta, "Hypervisor security- A major concern," International Journal of Information and Computation Technology, vol. 3, no. 6, pp. 533–538, 2013.
[27] Farahnakian F, Pahikkala T, Liljeberg P, Plosila J, Tenhunen H (2014) Multi-agent based architecture for dynamic VM consolidation in cloud data centers. In: IEEE 40th euromıcro conference on software engineering and advanced applications, pp111–118.
[28] Arroba, P., Moya, J.M., Ayala, J.L. and Buyya, R., 2015, October. DVFS-aware consolidation for energy-efficient clouds. In 2015 International Conference on Parallel Architecture and Compilation (PACT) (pp. 494-495). IEEE.
[29] A. Cleeff, W. Pieters, and R. Wieringa, "Security implications of virtualization: A literature study," in Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE '09), vol. 3, pp. 353–358, 2009.
[30] S. Jin, J. Seol, J. Huh, and S. Maeng, "Hardware-assisted secure resource accounting under a vulnerable hypervisor," ACM SIGPLAN Notices, vol. 50, no. 7, pp. 201–213, 2015.
[31] Gupta, P., Kulkarni, A. and Sarda, A., 2013. An embedded health care supervisory systems. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3, pp.379-386.
[32] S. N. Brohi, M. A. Bamiah, M. N. Brohi, and R. Kamran, "Iden- tifying and analyzing security threats to virtualized cloud com- puting infrastructures," in Proceedings of the 2012 International Conference on Cloud Computing Technologies, Applications and Management, ICCCTAM 2012, pp. 151– 155, are, December 2012.
[33] A. Ukil, D. Jana, and A. De. Sarkar, "A Security Framework in Cloud Computing," International Journal of Network Security and Its Applications, vol. 5, no. 5, pp. 11– 24, 2013.
[34] L. Adhianto, S. Banerjee, M. Fagan et al., "HPCTOOLKIT: Tools for performance analysis of optimized parallel programs," Concurrency and Computation: Practice and Experience, vol. 22, no. 6, pp. 685–701, 2010.