Sarwar *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0702151

Research Article

Vol. 7 issue 2 Year 2023

Optimizing Virtualization for Client-Based Workloads in Cloud Computing

Muhammad Imran Sarwar

Department of Computer Science & IT, The Superior University, Lahore, Lahore-54500, Pakistan

Corresponding author: info@imranchishty.com

Received: February 25, 2023; Accepted: March 09, 2023; Published: June 15, 2023

Abstract

Cloud computing has transformed the IT field by offering adaptable and versatile resources to cater to the increasing demands of businesses and organizations. Virtualization technologies are instrumental in facilitating the efficient deployment and management of resources within cloud environments. However, there are notable concerns regarding the security implications of virtualization in the cloud. This research paper thoroughly examines the security aspects of virtualization technologies in cloud computing, primarily focusing on identifying potential weaknesses, risks, and strategies to mitigate security threats. Additionally, the study investigates the security features and mechanisms provided by leading virtualization platforms and management tools. It scrutinizes access controls, isolation methods, network security, data protection, and integrity mechanisms offered by virtualization technologies to safeguard the cloud infrastructure and customer data. Furthermore, the paper addresses emerging security concerns associated with containerization technologies, encompassing vulnerabilities related to container escape, risks stemming from shared kernels, and issues concerning image integrity. It explores the effectiveness of container security measures, such as isolation, sandboxing, and access controls, in reducing these risks. Lastly, the paper summarizes the main findings and provides recommendations to enhance the security of virtualization technologies in cloud computing. It emphasizes the importance of continuous monitoring, regular security updates, robust access controls, and threat intelligence integration to mitigate security risks and uphold a secure cloud infrastructure.

Keywords: Cloud Computing, Virtualization Technologies, Security Analysis, Vulnerabilities, threats countermeasures, Hypervisor, Containerization, Access Controls.

1. Introduction

Cloud computing is a technology that enables users to access various services, applications, and data storage. It functions as a pool of resources characterized by two main features. The first characteristic is elasticity, which allows users to adjust and allocate

resources according to their specific needs dynamically. The second feature is multi-tenancy, which enables multiple users to access and store data on the same shared resources [1]. The primary goal of Software as a Service (SaaS) is to facilitate efficient enterprise or site search on the Internet. Quick and accurate access to information from databases and internal storage via website content is crucial in fast-paced organizations. As a search technology branch, SaaS provides significant benefits to various companies and external customers, catering to their specific requirements. Users access SaaS through a web browser, allowing them to manage, store, and process essential resources like software, operating systems, and applications in a cloud-based environment [2]. Platform as a Service (PaaS) allows clients to deploy and utilize diverse applications using programming languages, libraries, services, and tools to assist users.

Public cloud environments offer users easy access to computing resources, including hardware components (operating systems, central processors, memory, storage) and software (application servers, services). These public clouds primarily serve the purpose of application development and testing. In contrast, although more expensive than public clouds, private clouds provide an ideal solution for addressing security and privacy concerns within organizations [3]. Community clouds, unlike public clouds, provide cost-effective access without additional expenses. They enable multiple organizations to share computing resources. Hybrid cloud models combine private and public infrastructures and are often adopted by organizations to manage their IT infrastructure effectively [4]. Hybrid cloud architecture offers flexibility and cost-efficiency, making it a preferred choice for businesses and customers. Figure 1 illustrates the cloud model.

Figure 1: Cloud service models

Virtualization is a vital component in cloud computing, as it allows for isolating resources and services from physical infrastructure. Organizations are increasingly acknowledging the importance of cost efficiency and environmentally sustainable practices in their operations. Virtualization provides advantages such as increased capacity and initial cost savings. However, it also brings about high-security concerns. Figure 2 depicts a conceptual virtualization model.

Figure 2: Virtualization model

As virtualization gains practicality, new advancements and technologies emerge, each with advantages, disadvantages, and risks. Implementing these emerging virtualization technologies often poses challenges for project administrators and implementers. Virtualization encompasses various applications and executions beyond specific and centralized server systems. In today's context, virtualization is widely supported on readily available systems utilizing Intel architecture hardware. This is made possible by Intel Virtualization Technology, which offers hardware support for processor virtualization and facilitates advancements in virtual machine (VM) monitoring software. Consequently, the resulting virtual machine monitors (VMMs) can accommodate a broader range of legacy and future operating systems while maintaining high performance. Virtualization can be applied to hardware and software, and the progress in virtualization technology continues to evolve. Many organizations are adopting virtualization due to its cost-saving benefits, but it is essential to evaluate the associated risks. While server virtualization receives significant attention in the industry and literature, other areas of virtualization also need consideration [5].

1.1. Types of Virtualization

1. Storage virtualization involves consolidating physical storage from multiple devices into a centralized storage pool managed through a central console. This pooling of storage capacity enables software programs to identify available storage from physical devices and aggregate it into a virtual storage environment accessible by VMs. The virtualized storage appears as a unified storage entity, allowing read and write operations. In certain cases, even a RAID cluster can be considered a form of storage virtualization [6].
2. Storage virtualization offers numerous advantages, including increased productivity and enhanced security. It enables remote access, allowing users to work from any location and on any computer. This flexibility provides employees with convenience and resilience, enabling them to work from home or while on the move [7]. Additionally, storage virtualization helps protect sensitive data by storing it on a central server, minimizing the risk of loss or theft [8].
3. Server Virtualization: Server virtualization is the most widely recognized form of virtualization in the cloud. It offers benefits such as improved hardware utilization and application uptime. The main concept behind server virtualization is to combine multiple smaller physical servers into a single larger physical server to utilize the processor more effectively. Server virtualization can be further categorized into the following types:
4. Full Virtualization: In this type, the complete emulation of the real hardware allows the software to run an unmodified guest operating

system.

5. Paravirtualization: The software runs in a modified operating system as a separate system, but not in an unmodified form.
6. Partial Virtualization: This hardware virtualization may require software modifications to function.
7. Network Virtualization: This technology offers a virtual infrastructure that simplifies the administration of software and hardware resources within a network. It can be categorized into two types: external virtualization, which combines or divides networks into virtual units, and internal virtualization, where software incorporates network functionalities. External network virtualization is also referred to as virtual LAN [3].

1.2. Hypervisor

A hypervisor, a VMM, is a technology used to create and run VMs. It enables multiple operating systems to share a single host system and its hardware resources. The hypervisor, also called software virtualization, is responsible for partitioning and allocating resources such as CPU and RAM on the hardware [9]. There are two types of hypervisors:

1. Type 1: Native/Bare Metal Hypervisor: This hypervisor is installed directly on bare-metal hardware, functioning as a software layer. It operates independently and does not require a different operating system. Some level of external management is needed to oversee its operation.
2. Type 2: Hosted Hypervisor: This hypervisor is installed within an operating system. It runs as a software application on the host operating system, providing virtualization services. Examples of hosted hypervisors include VirtualBox and VM Workstation.

1.3. Virtualization Techniques

This technique depends on paired interpretation to trap just as to virtualize certain touchy and non-virtualizable guidelines with new arrangements of directions that have the proposed impact on the virtual equipment. The binary image is controlled at the runtime, and User level code is straightforwardly executed on the processor for superior virtualization. The mix of parallel interpretation just as immediate execution gives Full Virtualization as the visitor OS is decoupled from the essential equipment by the virtualization layer. Paravirtualization primarily alludes to correspondence between hypervisor just as visitor OS to improve productivity and execution. Paravirtualization additionally includes changing the OS part to supplant non-virtualizable Guidelines with hyper calls, which discuss straightforwardly with the virtualization layer hypervisor. Memory Virtualization. It familiarizes a course by decoupling the specialist's memory to give a passed-on, shared, or organized limit. It improves execution by giving more impor-

tance to memory limits without extension to the essential memory [10].

2. Related Work

[11] Storage virtualization refers to combining physical storage from multiple devices into a unified storage pool managed through a central control system. This allows software programs to recognize available storage from physical devices and merge it into a virtual storage environment that VMs can access. The virtualized storage is a single entity, enabling read and write operations. In some cases, even a RAID cluster can be considered a form of storage virtualization.

[12] The advantages of storage virtualization are significant, including increased productivity and enhanced security. It enables remote access, allowing users to work from any location and computer. This flexibility provides convenience and resilience for employees working remotely or while on the move [8]. Additionally, storage virtualization ensures the security of sensitive data by storing it on a central machine, minimizing the risk of loss or theft.

[13] Storage virtualization is the process of merging physical storage from various devices into a centralized storage pool controlled through a central console. This consolidation of storage capacity enables software applications to recognize and merge available storage into a virtualized storage environment that can be accessed by VMs. The virtualized storage is perceived as a unified entity, enabling read and write operations. In some instances, a RAID cluster can also be regarded as a type of storage virtualization.

[14] Storage virtualization offers numerous benefits, such as improved productivity and heightened security. It enables remote access, allowing users to work from any location and using any computer. This flexibility provides employees with convenience and adaptability, allowing them to work effectively from home or while traveling. Moreover, storage virtualization guarantees safeguarding sensitive data by storing it on a centralized machine, thereby minimizing the potential risks associated with data loss or theft.

[15] The presence of expensive and proprietary equipment, along with strict signaling protocols, poses challenges for current mobile core networks. When specific functionality is lacking, mobile operators are required to replace their hardware, even if it is sufficient for most purposes. This highlights the difficulty of implementing Network Function Virtualization (NFV) and emphasizes the need for dynamic designs to create and manage network capabilities. NFV's core concept revolves around deploying Virtualized Network Functions (VNFs) in a deployment diagram. The virtualization of the mobile core network using Cloud EPC can address the issue of costly control and maintenance of long-distance persistent tunnels for mobile operators. Technologies like MME pooling facilitate this approach. It's important to note that only a portion of the mobile core network can be virtualized if desired. Cloud EPC enables a

transition to a more intelligent, resilient, and scalable core architecture. By leveraging Cloud EPC, mobile carriers can expand their existing horizontal market business and explore vertical markets that were previously untapped. Service providers have the opportunity to offer home services through dedicated Customer Premises Equipment (CPE) supported by network-centric back-end systems.

[16] The VMM needs to offer a software interface to the VM that closely mimics the underlying hardware. However, it should also retain control over the machine and the ability to intervene in hardware access when necessary. When assessing these factors, the main design objectives for VMMs are compatibility, performance, and simplicity. Compatibility is of utmost importance because the key advantage of a VMM is its capability to run legacy software. Performance, which evaluates the effects of virtualization, aims to ensure that the VM operates at the same speed as software on real hardware.

[17] Virtualization improves the efficiency, ease of management, and reliability of centralized computer systems. It enables multiple users with different operating system requirements to effectively share a virtualized server. By coordinating operating system updates across VMs, downtime can be minimized. Additionally, failures in guest software are isolated to the specific VMs in which they occur. While these advantages have traditionally been associated with high-end server systems, recent academic research and the emergence of VM-based products indicate that the benefits of virtualization are applicable to a wider range of server and client systems. This cloud model emphasizes availability and encompasses five key attributes, three service models, and four deployment models.

[18] During the initial adoption of VMs, it was typical for a single organization to develop the VMM, hardware, and guest operating systems. These vertically integrated companies allowed experts to refine traditional virtualization techniques. One approach involved modifying guest operating systems to provide higher-level information to the VMM, taking advantage of the flexibility in the VMM/guest operating system interface. Another approach focused on exploiting the flexibility in the hardware VMM interface to enhance traditional VMMs. The VMM stored much of the privileged state of the guest in a hardware-defined structure and executed the SIE instruction to initiate interpretive execution. During interpretive execution, many guest operations, which would normally trap in a non-privileged environment, accessed shadow fields. Virtualizing the memory management unit (MMU) presented many complex scenarios when analyzing hardware VMMs. In this section, we explore future approaches in both hardware and software to bridge the performance gap with software VMMs. As hardware implementations advance, the overheads associated with hardware virtualization will diminish over time. Measurements were conducted on a desktop system using. It is important to note that for clarity, we have treated the software and hardware VMMs as separate entities. However, in VMware, both VMMs are part of

the same binary. We have conducted experiments with a hybrid VMM that dynamically selects the execution method based on heuristic algorithms driven by guest behavior. The goal is to leverage the superior system-level performance of the hardware VMM and the superior MMU execution of the software VMM.

[19] In NFV organizations, the task of assigning various administration chains to the physical network is essential. An administration chain comprises one or more services or virtual machines (VMs) interconnected to fulfill specific functionalities. These administration chains can be assigned in a hybrid network environment, utilizing either physical hardware or virtualized instances. When a service request is made, it can be allocated on dedicated hardware or through a VM provided by the service provider. Additionally, client VMs can be integrated into an administration chain. The main distinction between service and VM requests is that the client who initiated the service chain request manages the VM within the administration chain. Resource allocation for the first two deployment types resembles network-aware VM allocation in cloud environments, with the only difference being the consideration of CPU and memory requirements for VM deployment.

[20] In order to improve the networking performance of scaling up VMs, it is crucial to identify the specific system component that is causing limitations. To achieve this, we initiate an evaluation process that scrutinizes the four main systems involved. Through virtualization of the cloud platform, we enhance the availability of resources and enhance the flexibility of their management. This approach also leads to cost reduction by enabling hardware multiplexing and improves energy efficiency.

[21] The online nature of the cloud system exposes it to security issues commonly found on the web. Despite its differences from traditional computer systems, the cloud system can encounter similar security challenges. Security and data protection are major concerns in cloud computing. Traditional security issues like vulnerabilities, viruses, and hacking attacks can jeopardize the integrity of the cloud system and can have more severe consequences due to the nature of cloud computing. Unauthorized access by hackers and malicious intruders can compromise cloud accounts and steal sensitive data stored within cloud systems. Since data and business applications reside in the cloud center, it becomes crucial for the cloud system to implement robust security measures.

[22] A challenging and emerging development in cloud computing and data center architectures is NFV. As hosted applications in cloud systems increasingly have complex networking requirements, providers seek greater flexibility in managing the underlying infrastructure. This flexibility necessitates the redistribution of VMs, applications, and data storage based on the real-time status of the system. The complexity of this task requires advanced management techniques and the adoption of software-based approaches, particularly highly scalable and dynamic network virtualization methods. Network virtualization entails the separation of functionalities within

a networking environment by dividing the roles of Internet Service Providers (ISPs) into two components: infrastructure providers responsible for managing the physical infrastructure, and service providers responsible for creating virtual networks by pooling resources from multiple infrastructure providers and offering comprehensive connectivity services.

[23] Scaling resources manually by a human administrator may seem simple. Still, it is not a viable option considering the increasing cloud size and multiple web services sharing the same infrastructure and data. Automating resource allocation for web services becomes crucial, considering performance history, issues, SLA requirements, and resource security when scaling up or down. Such a system can rely on AI techniques to efficiently determine the required resources for the service. One commonly used machine learning algorithm is Support Vector Machines (SVM), employed in tasks like pattern recognition, spam filtering, and anomaly network intrusion detection. SVM can learn patterns and provide accurate classification by utilizing class labels. It finds the optimal global solution by finding a hyperplane that separates two classes. The data points closest to the hyperplane are known as support vectors, and based on their features, the predicted class is determined. In this study, a novel clustering selection algorithm has been proposed for collaborative range sensing. The algorithm focuses on selecting the most reliable cluster heads that can transmit their sensing decisions to the aggregation center. The scheme's performance has been evaluated by analyzing energy consumption and transmission delay, comparing it to the conventional model. Analytical and simulation results demonstrate the superior performance of the proposed method across different trust level values compared to the conventional model.

[24] Organizing unknown documents using ML techniques can be divided into two subsequent stages: training and testing. In the first stage, a designated set of documents, known as the training set, is provided to the system. Each document is then parsed, and a vector representing the document is extracted based on a predetermined vocabulary. These representative vectors and the corresponding known labels serve as input to a learning algorithm. By training on these vectors, the learning algorithm generates a classification model. To assess the performance of the computer processor, we utilize the sysbench stress test. This test is designed to challenge the central processor by calculating prime numbers. The algorithm divides the number using progressively increasing numbers and verifies that the remainder (estimate) is zero. In this particular case, we examine how power consumption increases as the number of virtual elements assigned to different physical cores increases, as explained in the context of computer pinning. This research paper provides a virtualization performance model for IT managers to follow before implementing Virtualization technology in their data centers.

[25] Virtualization allows existing operating systems to run on shared-memory multiprocessors. VMs can create diverse testing environments, facilitating innovative and effective quality assurance processes. Additionally,

virtualization can be leveraged to introduce new features to existing operating systems with minimal effort. It simplifies tasks such as system migration, backup, and recovery, making them more manageable and cost-effective. Virtualization provides a practical approach for achieving parallel compatibility across various hardware and software platforms, enhancing coherence among different aspects of the virtualization process.

[26] The cloud infrastructure is distributed among multiple instances operating within the cloud. When many VMs run on the same node, their performance can be negatively impacted. This is particularly evident when multiple machines are simultaneously utilizing the network, managing a significant volume of data. Similarly, access to the hard drive is shared among the virtual entities, and in the Amazon cloud, disk access, and network usage are treated as shared resources. The utilization of Mobile Edge Computing (MEC) systems also presents opportunities for further research in developing new services and applications to enhance network efficiency and improve the user experience. MEC can be leveraged to maintain network or service states for emerging applications, such as ensuring scalability by preserving critical parameters and providing backup support.

3. Proposed Methodology

The proposed methodology of this study is depicts in the Figure 3.

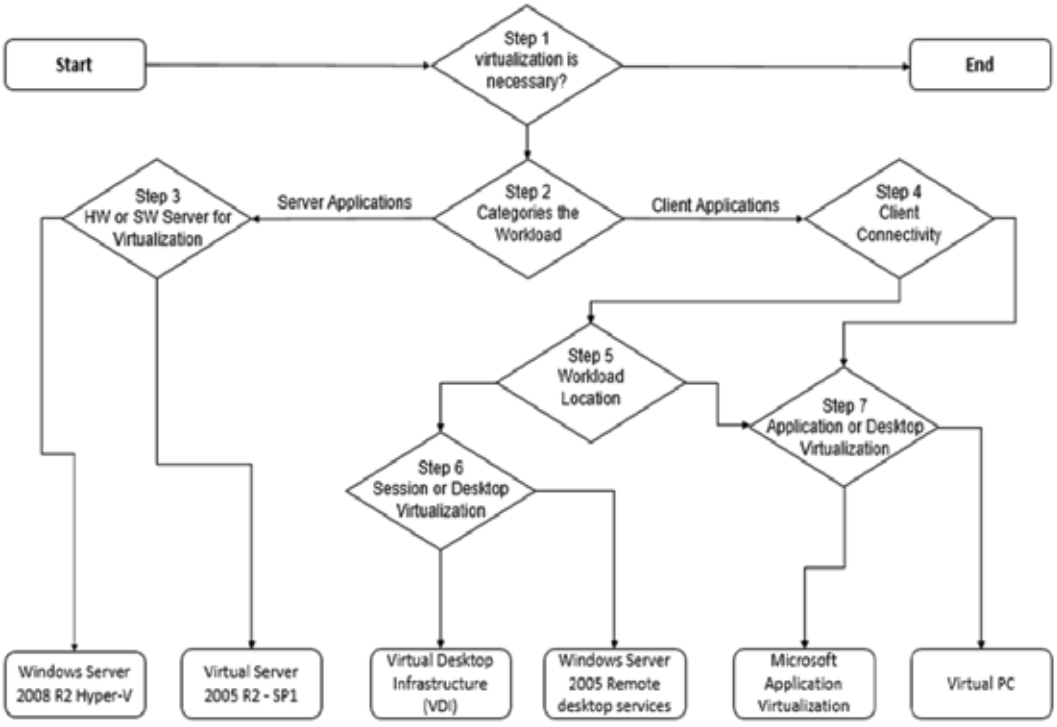

Figure 3: Research Methodology

Step 1: Is Virtualization Necessary:

This step aims to assess virtualization's suitability for a specific scenario. Several factors should be considered when considering virtualization to determine its compatibility with the needs. Compatibility refers to the ability of different components to work together [27]. Verifying whether the workload can be effectively executed in a virtualized environment is important. Workloads can include applications running on the client, server, or a combination. Susceptibility is another factor to consider. It involves evaluating whether the workload can run in a virtualized environment. It is advisable to review the support policies of non-Microsoft vendors to ensure compatibility across different virtualization technologies. Licensing is an important aspect to examine. It involves verifying if the necessary licenses are available to use the workload in a virtualized environment. Furthermore, it is crucial to determine the benefits of virtualizing the workload to the business. Assessing the business case for virtualization can reveal potential advantages such as cost savings, reduced implementation time, and low management costs [28].

Step 2: Categories the Workload:

Once the decision has been made to proceed with virtualization, the next step is to classify the workload into the appropriate category [29]. This step involves determining whether the workload is designed to run on a Windows Server-based server or a client device. Server workloads have distinct resource requirements and levels of interactivity compared to workloads specifically designed for server operating systems.

Step 3: Hardware Server or Software Server for Virtualization:

Microsoft provides two server virtualization products: Hyper-V, integrated into Windows Server 2008 R2, enabling hardware virtualization for servers, and Virtual Server 2005 R2 with SP1, offering software virtualization for servers [30]. The objective of this stage is to identify the product that best aligns with the specific technological needs of the environment for establishing most appropriate virtualization framework.

Step 4: Client Connectivity:

This step involves narrowing down the virtualization options based on the network requirements of the client computers. For server-based systems, computers already connected to the network can be utilized, whereas locally available applications will need to be relied upon for those not connected [31]. It is important to note that user specifications and application requirements can vary between different workloads, so the decisions made in this and subsequent sections should be validated for each workload being virtualized.

Option 1: Connected Clients, Option 2: Disconnected Clients

Step 5: Workload Location:

The subsequent phase for interconnected client

systems involves determining the execution location for the workload. Based on the previous technology choices, the virtualized workload can operate either in a centralized or decentralized manner.

Option 1: Workload Centralization, Option 2: Workload Decentralization

Step 6: Session or Desktop Virtualization: After deciding to centralize operations, the subsequent task involves choosing between session virtualization and desktop virtualization. In both scenarios, users establish connections to centralized workloads via a Remote Desktop Protocol (RDP) connection. Client computers can operate with a complete operating system and an installed RDP client, such as Windows 7 or any other compatible operating system [32]. Alternatively, they can be diskless and boot directly from the network, without storing any local data or programs.

Option 1: Virtualization of Sessions, Option 2: Virtualization of the Desktop

Step 7: Application or Desktop Virtualization: In this stage, the suitability of the workload for either application virtualization or desktop virtualization is determined.

Option 1: Virtualization of applications, Option 2: Virtual PC

App-V enables the installation of applications through MSI or on-demand streaming into a virtualized environment. In this setup, user machines are capable of handling application processing. To deploy and execute virtualized applications, client computers must have a compatible full client operating system that meets the hardware requirements specified by App-V. Additionally, a reliable network connection is necessary [33]. Windows Virtual PC allows users to run complete client operating systems on their local computers. The client computer must have sufficient CPU, memory, disk, and network resources for the base Windows operating system and each VM utilized to support this configuration. Windows Virtual PC facilitates the execution of legacy programs and operating systems, with Windows XP Mode in Windows 7 offering a tailored Windows XP VM running on Windows Virtual PC.

4. Simulations And Results

Checklist of items to consider:

1. Let's begin with the network.
2. Give the VM a name.
3. Choose a location for the VM.
4. Determine the VM's size.
5. Recognize the price model.
6. Storage for the VM.
7. Choose a computer operating system.

Figure 4 shows the Azure services interface.

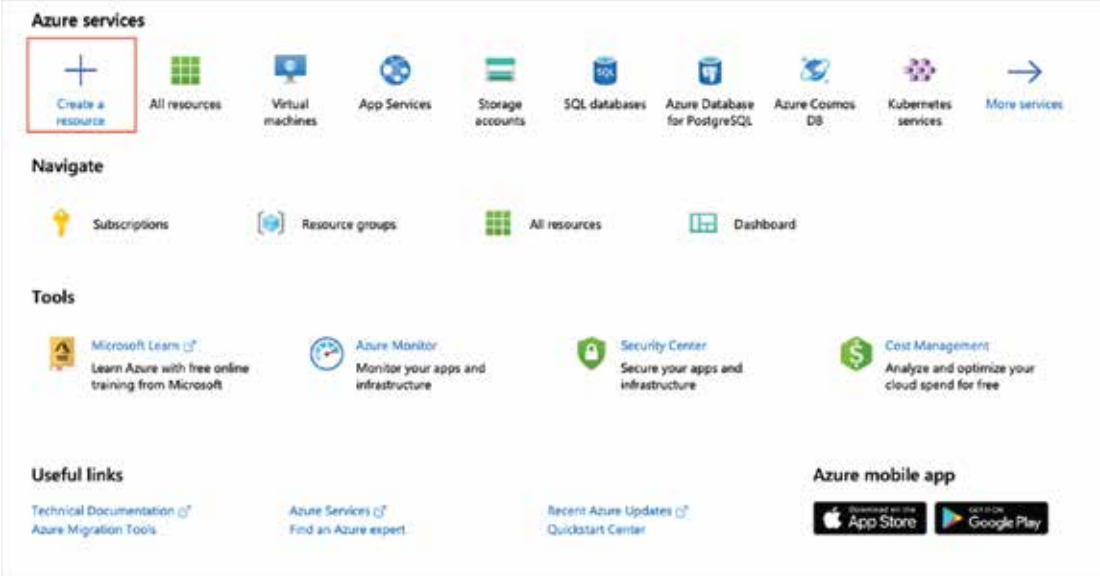

Figure 4: Azure services interface

Network: First consider the network, not the VM. Azure uses virtual networks (VNets) to provide secure connectivity between Azure VMs and other Azure services. VMs and services in the same virtual network can communicate [34].

Divide Network into Sections: Construct one or more subnets for the virtual network after choosing the virtual network address space(s). This allows to divide the network into more manageable portions. For example, that may give VMs 10.1.0.0, back-end services 10.2.0.0, and SQL Server VMs 10.3.0.0.

Keep the network Safe: By default, there is no inherent security boundary between subnets, allowing unrestricted communication between services. However, it is possible to establish Network Security Groups (NSGs) to control the flow of traffic to and from subnets and virtual machines (VMs) [35]. NSGs function as software firewalls at the network interface, enabling the application of customized rules to regulate inbound and outbound requests.

Plan for Each VM Deployment: Start with VMs that is to be built once it has mapped out with communication and network requirements. Selecting a server and taking an inventory is a good idea:

1. With whom does the server communicate?
2. What ports are available?
3. What operating system is being used?
4. How much disc space is currently occupied?
5. What kind of information is used in this? Are there any legal or other ramifications to not having it on-premises?
6. What is the server's CPU, memory, and disc I/O load like? Is there a need to account for surge traffic?

Giving Name to VM: The VM's name is one piece of information that many people overlook. The computer name configured as part of the operating system is the VM name. On a Windows VM, it can be given a name up to 15 characters; on a Linux VM, name can be given up to 64 characters [36]. In Azure, an Azure resource is a managed entity. VM, like physical computers in datacenter, require various components to function properly:

- Storage account for the discs in the VM
- Networking over the Internet (shared with other VMs and services)
- To communicate across a network, it needs a network interface.
- Secure network traffic with Network Security Groups Public Internet address

VM Location: Azure has servers and discs in data centers worldwide [37]. To offer redundancy and availability, these data centers are divided into geographic regions ('West US,' 'North Europe,' 'Southeast Asia,' and so on) - selection of VM location as shown in Figure 5.

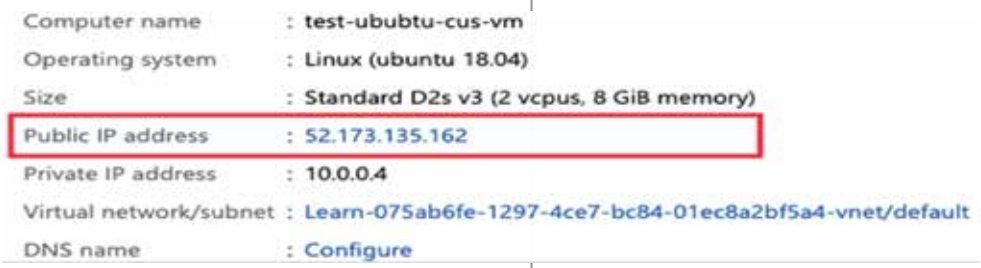

Figure 5: Location selection

Determine the VM's Size: After name and location have been decided, it will need to determine the size of the VM. Rather than specifying processor power, memory, and storage capacity separately, Azure offers a variety of VM sizes with different variants of these factors [38]. Azure offers a variety of VM sizes, allowing to choose the right combination of computation and memory.

Size Adjustment: When the current VM size no longer matches the requirements, Azure allows to adjust it. It can upgrade or downgrade the VM if the new size is compatible with the present hardware configuration [39]. This allows for a completely flexible and agile approach to VM management.

Select Price Model: The subscription will be charged two distinct costs for each VM: computation and storage. It may scale these costs independently and only pay for what is needed by separating them.

Storage for VM: All Azure VMs should have at least two virtual hard discs as a best practice (VHDs). The operating system is stored on the first disc, while temporary storage is kept on the second. Additional discs can be added to hold application data; the maximum number is governed by the VM size (typically two per CPU) [40].

Azure Storage: Microsoft's Azure Storage is a cloud-based data storage service. It can store practically any data, giving the secure, redundant, and scalable access. For a given subscrip-

tion, a storage account grants access to items in Azure Storage. Each attached virtual disc is always stored in one or more storage accounts on VMs [41].

Choosing a system: Different Windows and Linux flavors versions can be installed on the VM using Azure's OS images. As previously stated, the operating system will impact the hourly compute rate because Azure includes the cost of the OS license in the prices. It can be used the New-AzVM cmdlet to create a new Azure VM:

```
New-AzVm `
    -ResourceGroupName "TestResourceGroup" `
    -Name "test-wp1-eus-vm" `
    -Location "East US" `
    -VirtualNetworkName "test-wp1-eus-network"
    -SubnetName "default" `
    -SecurityGroupName "test-wp1-eus-nsg" `
    -PublicIpAddressName "test-wp1-eus-pubip" `
    -OpenPorts 80,3389
```

To create an Azure VM with the az vm create command:

```
az vm create \
    --resource-group TestResourceGroup \
    --name test-wp1-eus-vm \
    --image win2016datacenter \
    --admin-username jonc \
    --admin-password aReallyGoodPasswordHere
```

C# code to create an Azure VM using Microsoft. Azure. Management. Fluent NuGet package:

```
var azure = Azure
.Configure()
        .WithLogLevel(HttpLoggingDelegatingHandler.Level.Basic)
        .Authenticate(credentials)
        .WithDefaultSubscription();
// ...
var vmName = "test-wp1-eus-vm";

azure.VirtualMachines.Define(vmName)
WithRegion(Region.USEast)
WithExistingResourceGroup("TestResourceGroup")
WithExistingPrimaryNetworkInterface(networkInterface)
WithLatestWindowsImage("MicrosoftWindowsServer", "WindowsServer", "2012-R2-Datacenter")
WithAdminUsername("jonc")
WithAdminPassword("aReallyGoodPasswordHere")
WithComputerName(vmName)
WithSize(VirtualMachineSizeTypes.StandardDS1)
Create();
```

Snippet in Java using the Azure Java SDK:

```
String vmName = "test-wp1-eus-vm";
// ...
VirtualMachine virtualMachine = azure.virtualMachines()
    .define(vmName)
    .withRegion(Region.US_EAST)
    .withExistingResourceGroup("TestResourceGroup")
    .withExistingPrimaryNetworkInterface(networkInterface)
    .withLatestWindowsImage("MicrosoftWindowsServer", "WindowsServer", "2012-R2-Datacenter")
    .withAdminUsername("jonc")
    .withAdminPassword("aReallyGoodPasswordHere")
    .withComputerName(vmName)
    .withSize("Standard_DS1")
    .create();
```

5. Conclusion

In conclusion, the security analysis of virtualization technologies in cloud computing presents a comprehensive understanding of the key challenges and potential threats associated with adopting virtualization in the cloud environment. Through an in-depth examination of various virtualization techniques and their security implications, this analysis has shed light on the strengths, weaknesses, and best practices organizations should consider ensuring robust security in their cloud-based virtualized infrastructures. The analysis highlighted the benefits of virtualization, such as resource optimization, scalability, and cost-effectiveness. However, it also revealed several security concerns arising from the shared nature of virtualized environments, including the potential for information leakage, unauthorized access, and hypervisor vulnerabilities. These risks underscore the need for robust security measures to protect sensitive data and ensure the integrity and confidentiality of cloud-based services.

6. References

[1]. N. Tabassum, A. Namoun, T. Alyas, A. Tufail, M. Taqi, and K. Kim, “applied sciences Classification of Bugs in Cloud Computing Applications Using Machine Learning Techniques,” 2023.

[2]. M. I. Sarwar, Q. Abbas, T. Alyas, A. Alzahrani, T. Alghamdi, and Y. Alsaawy, “Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study,” IEEE Access, vol. 11, no. January, pp. 6490–6512, 2023, doi: 10.1109/ACCESS.2023.3237550.

[3]. T. Alyas, K. Ateeq, M. Alqahtani, S. Kukunuru, N. Tabassum, and R. Kamran, “Security Analysis for Virtual Machine Allocation in Cloud Computing,” Int. Conf. Cyber Resilience, ICCR 2022, no. Vm, 2022.

[4]. T. Alyas et al., “Performance Framework for Virtual Machine Migration in Cloud Computing,” Comput. Mater. Contin., vol. 74, no. 3, pp. 6289–6305, 2023.

[5]. T. Alyas, S. Ali, H. U. Khan, A. Samad, K. Alissa, and M. A. Saleem, "Container Performance and Vulnerability Management for Container Security Using Docker Engine," Secur. Commun. Networks, vol. 2022, 2022.

[6]. M. Niazi, S. Abbas, A. Soliman, T. Alyas, S. Asif, and T. Faiz, "Vertical Pod Autoscaling in Kubernetes for Elastic Container Collaborative Framework," 2023.

[7]. T. Alyas, A. Alzahrani, Y. Alsaawy, K. Alissa, Q. Abbas, and N. Tabassum, "Query Optimization Framework for Graph Database in Cloud Dew Environment," 2023.

[8]. T. Alyas et al., "Multi-Cloud Integration Security Framework Using Honeypots," Mob. Inf. Syst., vol. 2022, pp. 1–13, 2022.

[9]. T. Alyas, N. Tabassum, M. Waseem Iqbal, A. S. Alshahrani, A. Alghamdi, and S. Khuram Shahzad, "Resource Based Automatic Calibration System (RBACS) Using Kubernetes Framework," Intell. Autom. Soft Comput., vol. 35, no. 1, pp. 1165–1179, 2023.

[10]. G. Ahmed et al., "Recognition of Urdu Handwritten Alphabet Using Convolutional Neural Network (CNN)," Comput. Mater. Contin., vol. 73, no. 2, pp. 2967–2984, 2022.

[11]. M. I. Sarwar, K. Nisar, and I. ud Din, "LTE-Advanced – Interference Management in OFDMA Based Cellular Network: An Overview", USJICT, vol. 4, no. 3, pp. 96-103, Oct. 2020.

[12]. A. A. Nagra, T. Alyas, M. Hamid, N. Tabassum, and A. Ahmad, "Training a Feedforward Neural Network Using Hybrid Gravitational Search Algorithm with Dynamic Multiswarm Particle Swarm Optimization," Biomed Res. Int., vol. 2022, pp. 1–10, 2022.

[13]. T. Alyas, M. Hamid, K. Alissa, T. Faiz, N. Tabassum, and A. Ahmad, "Empirical Method for Thyroid Disease Classification Using a Machine Learning Approach," Biomed Res. Int., vol. 2022, pp. 1–10, 2022.

[14]. T. Alyas, K. Alissa, A. S. Mohammad, S. Asif, T. Faiz, and G. Ahmed, "Innovative Fungal Disease Diagnosis System Using Convolutional Neural Network," 2022.

[15]. H. H. Naqvi, T. Alyas, N. Tabassum, U. Farooq, A. Namoun, and S. A. M. Naqvi, "Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2533–2539, 2021.

[16]. S. A. M. Naqvi, T. Alyas, N. Tabassum, A. Namoun, and H. H. Naqvi, "Post Pandemic World and Challenges for E-Governance Framework," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2630–2636, 2021.

[17]. W. Khalid, M. W. Iqbal, T. Alyas, N. Tabassum, N. Anwar, and M. A. Saleem,

"Performance Optimization of network using load balancer Techniques," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2645–2650, 2021.

[18]. T. Alyas, I. Javed, A. Namoun, A. Tufail, S. Alshmrany, and N. Tabassum, "Live migration of virtual machines using a mamdani fuzzy inference system," Comput. Mater. Contin., vol. 71, no. 2, pp. 3019–3033, 2022.

[19]. M. A. Saleem, M. Aamir, R. Ibrahim, N. Senan, and T. Alyas, "An Optimized Convolution Neural Network Architecture for Paddy Disease Classification," Comput. Mater. Contin., vol. 71, no. 2, pp. 6053–6067, 2022.

[20]. J. Nazir et al., "Load Balancing Framework for Cross-Region Tasks in Cloud Computing," Comput. Mater. Contin., vol. 70, no. 1, pp. 1479–1490, 2022.

[21]. N. Tabassum, T. Alyas, M. Hamid, M. Saleem, S. Malik, and S. Binish Zahra, "QoS Based Cloud Security Evaluation Using Neuro Fuzzy Model," Comput. Mater. Contin., vol. 70, no. 1, pp. 1127–1140, 2022.

[22]. M. I. Sarwar, K. Nisar, and A. Khan, "Blockchain – From Cryptocurrency to Vertical Industries - A Deep Shift," in IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), September 20-23, 2019, Dalian, China, 2019, pp. 537–540. doi: 10.1109/ICSPCC46631.2019.8960795.

[23]. S. Malik, N. Tabassum, M. Saleem, T. Alyas, M. Hamid, and U. Farooq, "Cloud-IoT Integration: Cloud Service Framework for M2M Communication," Intell. Autom. Soft Comput., vol. 31, no. 1, pp. 471–480, 2022.

[24]. W. U. H. Abidi et al., "Real-Time Shill Bidding Fraud Detection Empowered with Fussed Machine Learning," IEEE Access, vol. 9, pp. 113612–113621, 2021.

[25]. M. I. Sarwar et al., "Data Vaults for Blockchain-Empowered Accounting Information Systems," IEEE Access, vol. 9, pp. 117306–117324, 2021, doi: 10.1109/ACCESS.2021.3107484.

[26]. N. Tabassum, T. Alyas, M. Hamid, M. Saleem, and S. Malik, "Hyper-Convergence Storage Framework for EcoCloud Correlates," Comput. Mater. Contin., vol. 70, no. 1, pp. 1573–1584, 2022.

[27]. N. Tabassum et al., "Semantic Analysis of Urdu English Tweets Empowered by Machine Learning," 2021.

[28]. N. Tabassum, A. Rehman, M. Hamid, M. Saleem, and S. Malik, "Intelligent Nutrition Diet Recommender System for Diabetic ' s Patients," 2021.

[29]. D. Baig et al., "Bit Rate Reduction in Cloud Gaming Using Object Detection Technique," 2021.

[30]. G. Ahmad et al., "Intelligent ammunition detection and classification system using convolutional neural network," Comput. Mater. Contin., vol. 67, no. 2,

pp. 2585–2600, 2021.

[31]. N. Tabassum et al., "Prediction of Cloud Ranking in a Hyperconverged Cloud Ecosystem Using Machine Learning," Comput. Mater. Contin., vol. 67, no. 3, pp. 3129–3141, 2021.

[32]. M. I. Tariq, N. A. Mian, A. Sohail, T. Alyas, and R. Ahmad, "Evaluation of the challenges in the internet of medical things with multicriteria decision making (AHP and TOPSIS) to overcome its obstruction under fuzzy environment," Mob. Inf. Syst., vol. 2020, 2020.

[33]. N. Tabassum, M. Khan, S. Abbas, T. Alyas, A. Athar, and M. Khan, "Intelligent reliability management in hyper-convergence cloud infrastructure using fuzzy inference system," ICST Trans. Scalable Inf. Syst., vol. 0, no. 0, p. 159408, 2018.

[34]. M. I. Sarwar, K. Nisar, S. Andleeb, and M. Noman, "Blockchain – A Crypto-Intensive Technology - A Review," in 35th International Business Information Management Association (IBIMA) Conference, November 4-5,2020, Seville, Spain, pp. 14803–14809.

[35]. M. A. Khan et al., "Effective Demand Forecasting Model Using Business Intelligence Empowered with Machine Learning," IEEE Access, vol. 8, pp. 116013–116023, 2020.

[36]. A. Amin et al., "TOP-Rank: A Novel Unsupervised Approach for Topic Prediction Using Keyphrase Extraction for Urdu Documents," IEEE Access, vol. 8, pp. 212675–212686, 2020.

[37]. S. Abbas, M. A. Khan, A. Athar, S. A. Shan, A. Saeed, and T. Alyas, "Enabling Smart City With Intelligent Congestion Control Using Hops With a Hybrid Computational Approach," Comput. J., vol. 00, no. 00, 2020.

[38]. M. Muhammad, T. Alyas, F. Ahmad, F. Butt, W. Qazi, and S. Saqib, "An analysis of security challenges and their perspective solutions for cloud computing and IoT," ICST Trans. Scalable Inf. Syst., p. 166718, 2018.

[39]. M. Mehmood et al., "Machine learning enabled early detection of breast cancer by structural analysis of mammograms," Comput. Mater. Contin., vol. 67, no. 1, pp. 641–657, 2021.

[40]. N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing," IEEE Access, vol. 7, pp. 174051–174071, 2019.

[41]. A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum, "Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management," Sensors (Basel)., vol. 22, no. 16, 2022.