ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse871032021.pdf
https://doi.org/10.30534/ijatcse/2021/881032021

Virtualization Security in Cloud Computing- A Survey

A. Rafique[1], Usman Nawaz[2], Namra Waheed[3], Muhammad Sama Yousaf[4]
[1]Department of Software Engineering, Foundation University Rawalpindi Campus, Pakistan, armalik001f20@gmail.com
[2]Department of Computer Science, Lahore Leads University, Lahore, Pakistan, usmannawaz065@gmail.com
[3]Department of Software Engineering, Foundation University Rawalpindi Campus, Pakistan, namrawaheed1997@gmail.com
[4]Department of Computer Science, Lahore Leads University, Lahore, Pakistan, msamayousaf59@gmail.com

ABSTRACT

Cloud computing at present is the most widely adopted computing paradigm across the globe. One of the core attribute of cloud computing virtualization is considered as selling point of cloud services. However, this cloud- based environment remains prone to hackers and intruders, prompting adverse effects on any computing system. Therefore, security is an important aspect of cloud computing considered as an integral part of virtualization. Paper aims to identify and explore issues transforming into challenges during process of virtualization presented through a survey of published literature. Paper aims to collect data from existing publications and present it in a useful format for fellow researchers to gain insight into this domain and have a comprehensive knowledge from a single paper. We have selected 40 papers to be included after careful analysis from existing literature till date form online digital data bases. We have classified the problems and with solutions in a matrix for ease of readers and help them in better understating our findings. We have also classified several tool and techniques in use of security of virtualization in cloud computing and their pros and cons.

Key words: Cloud Computing, Virtualization, Virtual Machines, Virtualization Issues and Challenges.

1. INTRODUCTION

Virtualization in terms of cloud computing is the method of abstracting computing resources in a single physical hardware sharable on multiple applications. In fact, it is creation of virtual resource version instead of real one. The agreed upon term "virtualization" is" server virtualization," where some physical server attributes are decoupled (abstracted) and replicated as vCPU, vRAM, vNIC, etc. in a hypervisor (virtualization software). In moments, these randomly assembled to create a virtual server [4].

Computing innovations have changed the technological scenarios by providing more and more convinces of organization at large to individuals since last decade. It is "Virtualization" executing important roles in managing and synchronizing available resource pool access to numerous virtual machines. These virtual machines run several diverse applications [1]. Virtualization is characterized as software that allows automatic partitioning of a single hardware calculating device to single or multi-assumed devices. It enables and enhances better use and control resulting in reduced cost, increased use of infrastructure and agility in speeding up virtualization processes [1]. Virtualization in cloud computing enables several VMs which are operating simultaneously on a single physical host machine (HM). Here, VM hosts the applications along with operating system, and middleware using hardware resource capacity partition [2]. Key features of cloud computing are a virtualization environment that allows device configuration as well as helps to build individual virtual machines. Virtualization extends accessible platform having intricate IT resources proving perfect to provide services. This technology allows abstraction of payload for application from the underlying physical resources at a basic level where physical resources may be modified as and when required into virtual / logical resources. This term is referred to as provisioning. Though, there are combined hardware environments, various management tools, regular patching and upgrading of programs, complex work- loads and multiple software architectures in the conventional approach. [1]

A. Types of Virtualization

Virtualization is currently divided into following types: -

1. **Server Virtualization**:

Various server virtualization implementations taking place. It is for wide range of platforms and architectures for CPUs. Familiarly, within a single physical system, server virtualization can be seen as the development of multiple virtual systems. We can take three methods to do this: OS Layer, Physical Layer and third is Virtualization Layer. Segmentation of hardware separates one physical server into segments where the operating system can be run through each partition, while the hypervisor puts a software layer between the physical hardware and the different operating systems which share the equivalent physical hardware.[8]

2. Storage Virtualization: Virtualization of storage has been there for numeral years. The usage of (RAID) i.e., redundant array of independent disks has begun. Using RAID, it is likely to group physical disks logically and provide those groups to the OS as a virtual disk. By using storage virtualization,

physical storage from multiple devices which will appear as a one storage pool be able to be combined. You may identify this storage as (DAS) i.e., Direct Attached Storage, (NAS) i.e., Network Attached Storage and Network Storage Area (NAS) (SAN). Using the Fiber Cable, Internet Small Computer Systems Interface (iSCSI) and Fiber Channel, Fiber Channel on Ethernet or Network File System Interface (NFSI), they can be connected (NFS).[8]

3)**OS Virtualization**: In Cloud Computing OS virtualization, the virtual machine program is installed on the host's OS instead of directly on the hardware system. The most critical use of virtualizing the operating system is to evaluate the program on multiple platforms or operating systems. The program is present in the hardware here, which facilitates the running of numerous applications. [8]

4) **Network Virtualization**: When people speak about network virtualization, Virtual Private Network (VPN) or even Virtual Local Area Networks are usually the earliest thing that arises to their minds (VLAN). The network virtualizations that are most used are: [8]

• Virtual Local Area Network or VLAN
• Virtual IP or VIP
• Virtual Private Network or VPN

B. Qualities -Virtualization

Characteristics of "Virtualization in Cloud Computing" and its environment have been appended below: -

1) Consolidation:

Virtualization removes the need for a single dedicated device for one program, and the same server can run multiple OSs. Both old and advanced OS versions can be installed on the same platform without buying additional hardware and new software can be run on their respective OS simultaneously.[1]

2) Easier development flexibility: Application developers can be able to run and test and check their applications and programs on the same virtualized machine in heterogeneous OS environments. It makes it easier to host a heterogeneous OS on virtual machines. The developers are also supported by isolating various applications in their respective virtual partitions.[1]

3) Migration and cloning: To manage the workload, virtual machines can be moved from one site to another. Users can use new hardware because of migration, as well as recover from hardware failure. In local locations and remote locations, cloned virtual machines are easy to deploy.[1]

4) Stability and security: Host operating systems host various types of multiple guest operating systems comprising many applications in a virtualized atmosphere. Each virtual machine is separated from each other and does not intervene in the function of the other at all, which in turn allows the feature of protection and stability.[1]

5) Paravirtualization: One of the significant aspects of virtualization is paravirtualization. With or without modifications, the guest OS will run on the host OS on a virtual machine. If any improvements or modifications are made to the operating system to be familiar with the Virtual Machine Manager (VMM)," Paravirtualization" is said to be this process.[1]

C. Virtualization Methods

1) Operating System-Based Virtualization: Virtualization is allowed on a single physical server by a host OS that supports several isolated and virtualized guest OSs by the feature that they are all on the similar kernel of the OS with exclusive hardware infrastructure power. Host OS is capable to sight virtual machines and has control above them. This method stays quick, but it has weaknesses, i.e., when an attacker inserts scripting control into the host OS, allowing every guest OSs on this kernel to get control of the host OS. The outcome is, all VMs which exist or will be created in the forthcoming will be regulated by the attacker.[3]

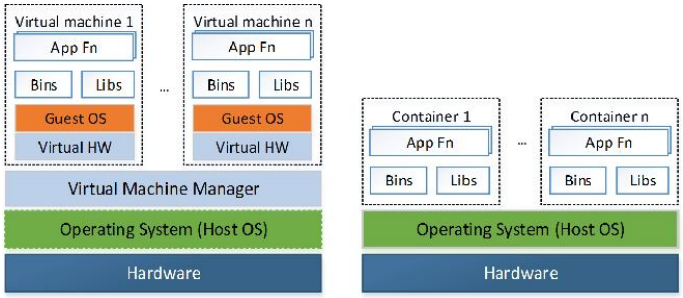

Fig. 1: Operating System-Based Virtualization

2) Application-Based Virtualization:

An application-based virtualization is hosted on the top of hosing OS. Individually VM with its own guest OS system and associated applications is then emulated by this virtualization program. In business environments, this virtualization architecture is not widely used. This approach's security concerns are close to operating system-based issues.[3]

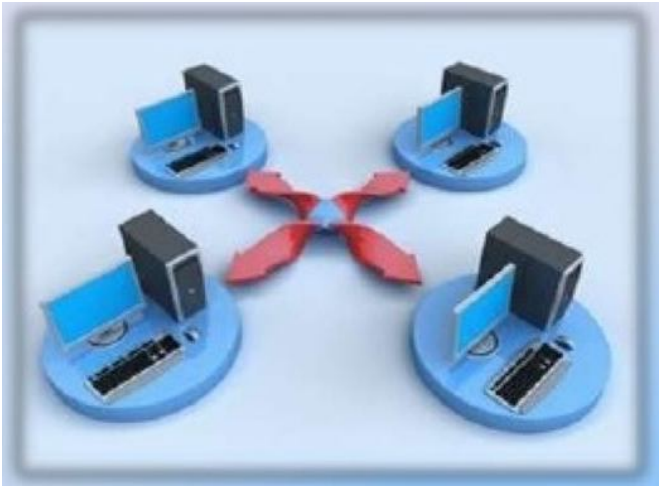

Figure 1.1- Application Virtualization

3) Hypervisor-Based Virtualization: To monitor the sharing of device resources across multiple VMs, the hypervisor is accessible at the machine's boot time. Of these, VMs are privileged partitions that control the Virtual Machines that are hosted and Virtualization Platform. Privileged partitions sight and monitor the Virtual Machines in this architecture.[3]

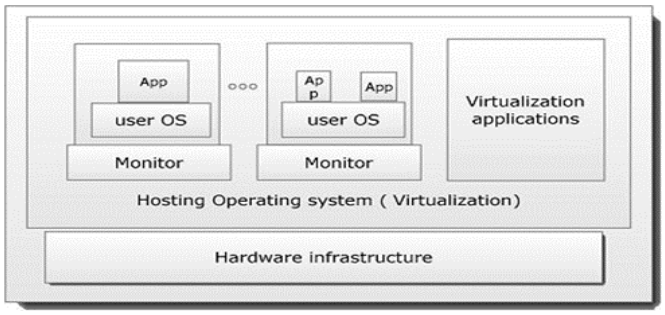

Fig. 2: Operating System-Based Virtualization

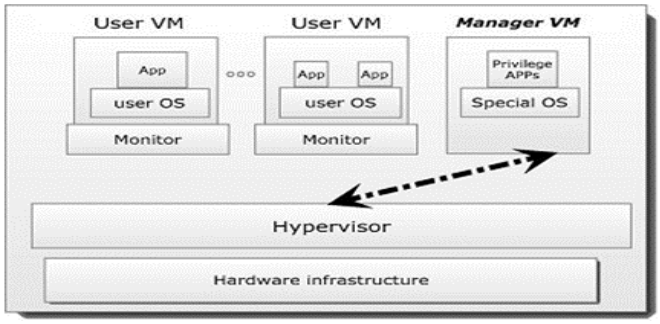

Fig. 3: Operating System-Based Virtualization

D. Relation between Virtualization and Cloud Computing

At the point when an end-client utilizes a PC, a view gave by the OS that abstracts all the accessible actual segments is the thing that he/she really talks with. The consumer acquires data from the point of view that he is interested in. It might be characterized that what virtualization organizes is to create a rare distinct physical machine logic interpretation, each of which can be used to communicate with a user concurrently. Virtualization is responsible for the cloud computing specifications for lively cutting and delivery of calculating resources. Virtualization requires creating an isomorphism that maps a real host to a virtual guest system. The guest state is mapped to the host state by this isomorphism. Virtualization produces plural subsets logically from the full set of machines from the resource angle. Every conceptual view can have a physical view of the comparable architecture. He/she does not essential to recognize whether the view is a visualization of physical assets or just a diagram of a logical collection of assets when a user interrelates with those assets through a view. End users do not see resource specifics, but simply pay devotion to and connect with the logic view given by the virtualization layer or VMMM layer. These subgroups are called VMs, which behave like real machines. Thus, the storage of the virtualization layer of services would be Constructed as a logical unit pool of open tools for the users, and software must bundle a collection of computing resources and behaviours on the virtual resource layer and present it as an available computing environment at the heart of what building a virtual machine means. Cloud based organizations are based on the service layer, in which, like P2P networks, the nodes are completely decentralized.[5]

E. Virtualization Security Framework

Two areas of virtualization security may be investigated: virtual machine security and security management of virtualization. In the chart below, a virtualization protection framework has been given. The security architecture for virtualization is efficiently organized into two sections, i.e., security management for virtualization and virtual machine security. Without disrupting each other, two modules perform their duties, so that the entire framework can be more functional. There are three levels of virtual machine security: The first layer is Physical Resource. VMM is the second layer, the more critical layer that must be greatly facilitated by protection mechanisms to safeguard running VMs. The VMs is topmost layer, which assist customers with virtualization services.[11]

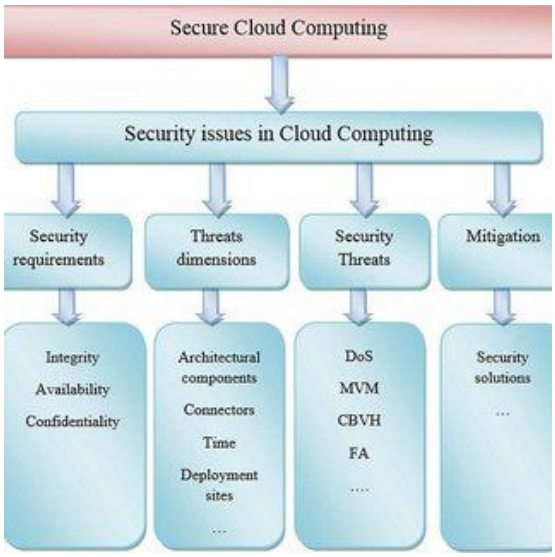

Figure 4- Virtual Security Framework

Research Questions

RQ1: What are emerging security challenges along with solutions in case of virtualization in cloud computing found in literature?

RQ2: What security issues confront and what are remedies found as per literature for virtualization in cloud computing?

RQ3: What security attacks are being confronted virtualization of cloud computing and what are possible ways to tackle them?

RQ4: How security vulnerabilities are checked, and solutions are sought?

RQ5: What are security threats and different tool and techniques in vogue to address these threats in Cloud Virtualization?

2. LITERATURE REVIEW

Farzad (2012) has defined some virtualization risks, attacks, and problems in cloud security i-e Virtual machine level attacks, DDOS attacks, extended network attack surface, client attack client, etc. and then proposed new security architecture for the hypervisor-based virtualization technology to protect the cloud environment and added some virtualization architecture features to improve sec. Moreover, two key units of the architecture proposed are based on this fact. The VM can be a target or an intruder when the amount of work of the VM increases unusually. The proposed architecture is the best attempt to decrease the workload, decentralize hypervisor and VM security-related functions, and transform the centralized security system to a distributed one. A distributed security framework is a very good way to reduce the hypervisor-based virtualization workload, but this distribution will insert cloud vulnerabilities. [3]

Yuping (2012) at al has stated that Cloud computing produces not only simplicity and performance advantages, even with the use of virtualization, there are also major problems in data storage and privacy protection. Several risks in virtualization are described in this paper i-e sabotaged of sabotaged host and network. Several approaches to increase the security of cloud computing are suggested to solve this issue, i.e., from the sole point of view that technology is not sufficient even to resolve the security of cloud computing, it also requires collaborative efforts to achieve the aim by the department of Information Security, the industrial sector, and the necessary department of government. [5]

Kazim (2012) at al has stated about various facets of the security of cloud virtualization have been discussed. They have established cloud computing virtualization protection criteria so that can be seen as a path towards protecting cloud virtual networks, cloud virtual infrastructure attacks and protection strategies to safeguard the virtualization system by resolving future threats and attacks [6]

Keiko [2013] et al identified the key weaknesses in cloud virtualization framework. It enumerated leading substantial threats. Its relevant literature along with detection and correlation of weaknesses with threats having potential answers. Other than cloud computing, there are no proper solutions for traditional data hosting including web apps. Author pointed out security issues for IaaS, PaaS, and IaaS. These issues keep on varying depending on the platform, virtualization, Storage, and networks. It is elaborated those issues emerge due to different paradigms, different technologies used and dealing with different security models and ways. Another difficulty is that there are numerous kinds of technology for virtualization, and every type will address security mechanisms in different ways. Virtual networks, especially when communicating with remote virtual machines, are also the target of some attacks. Surveys have tackled cloud security concerns without making any distinction between weaknesses and threats. We have concentrated on this distinction, where certain problems are considered necessary to understand. It was not sufficient to list these security problems; that is why we have constructed a link between threats and weaknesses so that we can recognize which weaknesses lead to the execution of these threats and make the framework more resilient. To handle these risks, some existing solutions have also been identified. New security techniques as well as redesigned conventional solutions that can work with cloud architectures are necessary, however. In cloud environments, conventional protection frameworks could not function well because they are a difficult architecture consisting of a variety of unlike technologies. [7]

Nagesh1[2013] et al has stated that in the information technology world, virtualization is a built-up utterance. Its ever infrastructure is reduced within data centers linked to other significant topics virtualization technology, such as ease its use and scalability, was recognized in advance not only by IT experts, but also by administrators and managers. The increasingly rising rate of acceptance of this technology has exposed these systems to new security issues that have been ignored or merely overlooked in recent history. At present, the author has provided a detailed state of the art view of Some of the old reasons for server virtualization, moreover a published explanation analysis contained inside this virtualization technology on various security issues. These issues can be realistic for all current virtualization technologies that are accessible without any emphasis on a particular response. Nevertheless, two of the mainstream accepted virtualization responses are prone to investigation: VMware ESX and Xen. In conclusion, several reasons as to how to enhance the protection of using virtualization for online banking and electronic commerce are illustrated. This paper is the outcome of research effort on virtual machines, and their key features and variances, and the effect of their use on defense. The usage of virtualization has many benefits, as well as reducing the required hardware resources with a direct cost effectiveness delivering security benefits additionally. Due to this advantage of security, it is widely used and is practiced largely. Desktop security has often raised some apprehensions for IT managers and end users who have been infected with viruses, larvae, or their identifications by a key logger or phishing attack. [8]

Naim (2017) et al illustrates two of the main cloud computing technologies are focused on security solutions for web services and virtualization. In comparison with the security as a service concept, the new concept of incorporating multiple level security into entire cloud offerings is also clarified. Safety issues found in the literature were then investigated. More conventional issues are primarily web services and others are more concerned with the introduction of cloud technologies such as cloud infrastructure, virtualization, cloud deployment models, service level agreements and cloud service models. These issues are mainly circled around two key categories first. In addition, the classification model of security problems was provided to assist in the control and in resolve of security issues. The security solutions and recommendations offered by the CSA and OWASP were formerly registered in the field of virtualization and web

services, along with the Amazon Web Services technique to protect hypervisors. In comparison to the popular security-as-a-service model, this paper also introduces the idea and significance of multi-level integrated cloud security and focus on the push model from CSP1, CSP2 to CSC to enforce security. In addition, significant guiding principles have been discussed for the creation of service level agreements. [9]

Ankur (2013) et al has described that to boost the features, in particular multi-tenancy and virtualization, cloud computing should be combined with many technologies and architectures; but they add their own security issues to the already wide list of cloud computing. Virtualization comes with its own problems as a multi-tenant, the hypervisor presents a new attack surface to be compromised; and the virtual network allows a malicious VM to carry out attacks on other VMs, ignoring conventional controls of network security. This involves a new way of approaching network security, such as using privileged VMs, but if compromised, this often poses new security risks. "CSA accurately states that" all tenants in the multi-tenant virtual world will share the lowest common security denominator un- less a new security model can be achieved that does not" wire" any network reliance for safety. For many organizations, the switch to the cloud could indicate an increase in security. To ensure proper protection with de-parameterization and to comply with the stricter regular laws and regulations, new stringent security controls would be required. [10]

Asvija (2019) et al has stated that Virtualization technology's benefits have led to its widespread acceptance in cloud computing infrastructures. It is however, implemented a completely unique collection of threats to security that are extreme in nature. Many of those threats are special and not applicable to conventional computing scenarios in virtualized environments. Thus, these risks have been less researched and therefore less discussed by maximum security application providers. For this purpose, it is essential to cautiously examine the various threats presented by diverse virtualization components and therefore effectively develop solutions to protect the systems against them. This study seeks to point the major weaknesses and expose readers to the numerous current attacks related to hardware-assisted virtualization, as it has become the most used method of virtualization in the construction of large data centers and cloud infrastructures today. For assessing the risks related with the threats listed, a Bayesian Attack Graph model is provided. A thorough discussion of the different counter measures suggested against the threats listed is discussed along with the list of difficulties in their adoption. [12]

Xiangyang (2011) has proposed a new solution, based on the divide-conquer strategy is proposed for the virtualization security problem introduced by cloud computing, especially for private cloud computing. First, the security risks caused by virtualization are evaluated and categorized, and then some corresponding solutions are proposed for each category of security risk based on the divide-conquer principle. Risk analysis demonstrates that the security threats of private cloud computing virtualization can be constantly minimized based on the suggested solutions in this paper. [13]

Chirag (2016) has described that in current virtualization implementations, different vulnerabilities are present, and there are thus different security issues at the virtualization layer. In this paper, the author studied various cloud computing virtualization layer vulnerabilities and attacks. This paper discusses Cloud Detection Mechanism and System Mechanisms for Intrusion Detection and Prevention proposals, and then suggests the criteria and scope of research for cloud IDS to achieve the required level of protection at the cloud computing virtualization layer.

Malhotra (2014) said that virtualization i.e., mass data loss, infected application and data integrity problems were described along with the advantages of virtualization i.e., isolation, resource sharing, dynamic resource, resource aggregation and isolation. [15]

Manjeet (2016) has described that Virtualization allows cloud computing to virtualize assets specifically for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service distribution. In computing, several virtual machines are used to provide cloud resources with versatility, agility and scalability that allow their virtual machines to be manipulated. Virtualized computing provides the client with access to resources at remote locations on digital machines. The features of resource management, hardware, operating system, and software isolation are supported by virtualization. Virtualization offers multi-tenancy capabilities for simultaneous access to virtual machines that are assigned to machines on a single physical computer. It is possible to build, copy and migrate virtual machines, this versatility contributes to security challenges. The purpose of this research paper is to highlight problems of legacy and new protection with feasible solutions. The privacy policy must be established in accordance with the user's specifications. This paper is a way of analyzing security loopholes and providing feasible alternatives to researchers. An undefeatable protection mechanism is still inaccessible in a virtualized physical machine, however. Researchers continue to function dramatically in this stream. As the technology of virtualization is still in its early days, it is still important to overcome several security loopholes. [16]

Daniele (2016) elaborated vastness of virtual technology. It enables cloud service providers to this computation power having advantages of being efficient, maintainable and expense. Putting it at disadvantage, attackers have also exploited virtualization by inventing innovative methods jeopardizing to breech in systems. In parallel with security threats, innovative ways used by hackers, numerous solutions have been explored and implemented dealing this security menace. People proved successful in providing solutions. Author has elaborated a war of tug between violators, hackers, and attacker verses individuals of science nullifying their malicious efforts through security measure and methods. Author reproduced security measures and methods encountering threats non existing before. It is also a matter of fact that these enhancement in virtualization, brought in new

threat regime and its complex response. Innovated complexity to create and manage security strategies has evolved. These strategies evolve threat, associate requisite security measure to achieve trust assumptions. This is done by categorizing threats in models. Detecting chances of attack on likely layer having focus on hardware, virtualization, OS, and application. A separate taxonomy of likely security attacks along with loopholes for intrusion have been identified and mentioned. Threat models are deliberately defined and presented as a structure and introduced new defense system approach for clarity of threats, to achieve precision in security, best possible trust in assumptions. All this enable author to present a set of methodologies for reliable security through classifies strategies in field of cloud computing with emphasizing virtualization after implementation [17].

2. DISCUSSION AND RESEARCH OUTCOME

DEEPIKA et al has contemporary presentation of a new technique called "skewness,". It is aimed at measuring unevenness regarding a server's usage on multi- tier resources. Through this optimizing Skewness, we feed adequate several types of workloads and thereby increase the entire consumption of server resources. It will lessen the time needed by this method. The author has presented an approach to the implementation and evaluation of a cloud computing service resource management system. Our paper also shows how we can effectively multiplex virtual resource allocation to physical resource allocation on fluctuating needs and use the skewness metric to better evaluate different resource characteristics such that server adequacies are well used. For systems that accept multiple-resource constraints, we may apply our algorithm to optimize both burdens and Green Computing.

Chu-Fu et al has developed Cloud computing systems' Energy Conserving Resource Distribution Scheme with Prediction (ECRASP). In the near future, the prediction mechanism will forecast the pattern of arriving jobs (dense or sparse) and their related characteristics, so as to assist the system in making acceptable choices. The results of the simulation indicate that our proposed ECRASP approach performs well in energy efficiency comparisons compared to traditional re- source allocation algorithms. The results of the simulation show that our proposed system can arrange for suitable PMs to arrange each arrival job and can make reasonable decisions about when to shut down a PM or start a new PM to save power consumption.

Kruekaew et al main contributed through their work by examining difference in the algorithm required for load balancing of VM. This results in reduction of time interval required for processing data. Using CloudSim instruments, the scheduling technique was simulated. As per results of experiments it became evident that combination of the proposed ABC algorithm is task size-based on scheduling where "Longest Job First" (LJF) scheduling algorithm provided a better performance scheduling strategy to change the environment and balance workload. It can reduce the time span of data processing. Author has implemented an ABC optimization algorithm that can solve the management of virtual machine scheduling in the light of environmental changes in the number of VMs and cloud computing requests. Cloud computing must be run on a stable infrastructure, even in changing environments. Therefore, for the cloud computing world, the ABC algorithm is ideal because the algorithm can use the increased machine resources efficiently and reduce the make-up span. The experimental results showed that ABC LJF's proposed techniques performed efficient results than all techniques and scalability is more prominent in its efficiency. The load balancing algorithm should be performed using the ABC-LJF algorithm to preserve system reliability and scheduling and to avoid the system crash in the event of increasing or decreasing the number of servers.

Saraswathi et al has replicated DC (datacenter) having two hosts having couple of Pes. Authors used CloudSim and produced two VMs in need one PE each. VMs are designated as hosts based on the number of available PEs in the host and the number of required PEs in the VM. Jobs are delivered for execution to the VMs. Based on the First Come First Serve basis, the first two jobs are assigned to the VMs. Checking the deadline for the next task. If it has a short term than the first two jobs, so it is a high priority job. The work is otherwise a low priority job. After all the workers have finished their execution, the low priority work must be executed. Each of the jobs in execution should be suspended for the success of high priority tasks. Checking the next task's deadline. If it is a short-term job than the first two, that is a high priority job. Otherwise, the job is a low priority job. After all the employees have completed their execution, it is important to conduct the low priority jobs. For the performance of high priority assignments, each of the performed jobs should be suspended.

Pandaba et al have discussed that a simple step towards achieving an efficient scheduling model is the Modified Round Robin algorithm. Scheduling algorithms do not impact the system's behavior (same results regardless of schedule). The algorithm does, however, affect the efficiency and response time of the system. The time quantum is the bottleneck facing the round robin algorithm, and solutions were questioned more frequently. Given the feasibility and usefulness of the Round Robin algorithm, this paper offers an answer to this question by using a dynamic quantum of time instead of a fixed quantum of time. To score a goal, it will require even more time and analysis.

Padmavathi et al has introduced a new Load Balancing Algorithm inspired by the Ant Colony Method has been proposed. To apply Elasticity, Dynamic Existence, We Developed Algorithms. The Open Source CloudSim Simulation Tool kit tested our proposed algorithm. Experimental studies have shown that the Proposed Average Make Period Algorithm is lower than current algorithms. Over 10 Runs, Standard Deviations are also compared.

Usman et al has proposed the ISA-based energy-efficient VM allocation technique aims to reduce the energy usage of the datacenter and increase the resource efficiency of physical resources. Models and the pseudo code of the Algorithm were developed. The world of Cloudsim was used as a test bed to simulate our algorithm. We show that after being compared with GA and BFD, our methodology is more effective in terms of energy usage and resource utilization. The findings show that GA and BFD energy consumption is 90 percent - 95 percent compared to the EE-IS proposed, which is about 65 percent. On average, 30 percent of energy was also saved using EE-IS, which has also increased the usage of resources.
Samson et al have revisited the topic of cloud computing resource allocation and the proposed binding HABBP strategy as a new and optimal approach to the problem of virtual resource allocation. To maximize the overall execution time of completing on-demand user requests, HABBP uses a load balancing policy for binding cloudlets to virtual machines in such a way that each cloudlet is assigned to the required virtual machine. We developed an optimization model, proposed HABBP, simulated in CloudSim both HABBP and traditional binding policy, and benchmarked these solutions against the algorithm of Simplex.
There is a Toolkit that is used to decrease the security of problems that may be happening in interoperation. These security problems are decrease without the interference of brokers. The toolkit is called the interoperation toolkit. If the toolkit is used it does not provide some cloud services.
The concept of integrating data in MCC with mobile clouds was discussed by Marco Scarpa and Riccardo Di Pietro [25]. ARIANNA -a software program-primarily based program as opposed to the software program regulations that let in "Secure Storage as a Service (SSAA S)" in MCC. Some of the cloud services like Open Stack Swift, Dropbox, and Google clouds are compared with quantitative performance analysis with multi-cloud technology given by Arianna's application.
Saleh et al has described that cloud computing data center, the pool of VMs must be Managed to maintain service quality and resource efficiency with an effective task scheduling algorithm. VM failure clearly reduces overall device throughput. This problem can be resolved through a process of VM recovery that allows VMs to be cloned to another host. When allocating resources for urgent work, VM migration should be considered because the transfer of a huge amount of data belonging to a VM will decrease overall efficiency.
Shuang et al has proposed a LCGA algorithm to accomplish scheduling tasks with lower costs of completion and load balancing. At the same time, the paper not only brings variance to reflect the load among computing workers, but also weights the function of multi-fitness. Experimental results show that the proposed algorithm takes little to complete the total task cost, and effectively balances the entire load of the system.
Shandong et al proposes the method of cloud resource assignment supports unexpected and pressing requirements, that can assign numerous resources in a convenient and efficient manner for critical resource requests. To assign resources prior for urgent virtual machine requests, this approach rebuilds current resource allocation needs. And a mathematical model of multi-objective optimization is developed, which sets the least output match distance among virtual and physical machines and the least number of physical machines as the resource allocation objectives. To solve this model, then, a multiple-objective optimization procedure is used. We are performing an experimentation to illustrate our approach. The early experimental findings indicate that our methodology has a definite benefit in minimizing the number of physical devices used and improving the usage of energy.
The upgrades of decision constraints optimizations trouble address the adopted method had a few troubles in discovering the most accurate solution. The computing experiments that compare different algorithms with branch and the bound algorithm have given the results that all previous algorithms are slow and branch and bound algorithm is fast, this all is discussed. Almothana et al presents a genetic algorithm-based scheduling technique. This strategy calculates in advance its effect on the system after the distribution of the necessary VM resources in accordance with the historical data and the current state of the system. The experimental results indicate that the strategy offers a better distribution of loads and decreases dynamic migration.

Research Outcome

1. We have studied literature from a broad angle when searching for articles, considering different aspects.
2. To develop a common method to be practiced in a specific context, researchers have made a great contribution.
3. There are countless computing fields currently operating and being taught and researched worldwide these days. Cloud computing is often adopted in a large range of areas, so compared to others, it has separate ramifications in a specific area.
4. Through having massive computational resources and being able to manage complex software capabilities to handle large computations as well as large computations, cloud computing has introduced a revolution in the field of computing.
5. Research indicates that there are number of various issues, challenges, risks, attacks, vulnerabilities, and threats involve in the security of virtualization in cloud computing.
6. There are multiple solutions which are proposed in research for these issues, challenges, risks, attacks, vulnerabilities, and threats.
7. We have done categorization for different issues, challenges, risks, attacks, vulnerabilities and threats and their solutions which are showing in Table-II and Fig-III

8. There are several tools and techniques which been designed and followed by software practitioners around the globe. Every technique has its own pros and cons depending upon the which tool will solve our problem
9. We have also done categorization for various tools and techniques being used in virtualization in cloud computing which are as below and shown in Table-I
    a. CloudSim simulator
    b. Green Cloud simulator
    c. Java

Table-I Tools and Technique

Serial No	RS ID	Use of Tool/ Technique /Approach	Outcome as Gains
1	18	Used "skewness approach to quantify the use of resources on the server and provide dynamic allocation of resources by minimizing burdens and Green Algorithm Computing".	•Satisfy needs of VM •Saves server resources
2	19	Proposed a Cloud Computing ECRASP Algorithm (Java)	•Safeguard VMs Power Consumption
3	21	CloudSim Simulator.	•Reduce overhead in executing all jobs
4	20	CloudSim Simulator. Optimizations of ACB Algorithm and its application.	•During Fluctuating Situations, ABCLJF Lowers the Make Span •Keeps system stable
5	22	MATLAB. Round Robin Scheduling Algorithm	•Reduction of total (on various systems) • Wait time • Turnaround time
6	25	CloudSim Simulator with HABBP Algorithm	•In terms of job total execution time, job • HABBP performs better • Outperforms CloudSim Simulator's conventional binding policy
7	23	CloudSim Simulator: DEACOLAB Algorithm	• In case of Make Span decreases • Average Deviation • Standard Deviation
8	24	CloudSim Simulator: EE-ISA	•Effective usage of resources •Reduced energy consumption •Saves 30% energy inside Data Centers
9	26	Green Cloud Simulator: 1. Use PSSA 2. Green Algorithm (Virtualized VM)	•Performs better in Virtualized Data Center System by handling load

Table-II Categorization of Issues

S/N	Categories					
	Vulnerabilities	Challenges	Risks	Threat	Attacks	Issues
1	Virtual Machines	Inter-VM Attacks	Risks of Virtualization	Virtual Machine	Virtual Machine Attacks	Data Leakage
2	Virtual Machines Images	Mixed Trust Level VMs	Risk of Resource Access Control	Channel Attacks	DDOS Attack	Data Remanence
3	Virtual Network	Resource Contention	Risk of DOS Attack	Memory Attack	Service provider	Data Breach
4	Hypervisors	Lack of Audit Trail	Risk of virtualization Platform in Building Network	-	Hypervisor	-
5	VM Escape	Data Integrity	Risk of virtualization Platform's Security Management		Guest Images	-
6	Denial of Services	-	-	VM Escape and VM Hopping	-	-

Table-III ProposedSolutions

S / No	Proposed Solutions				
	Risks	Vulnerabilities	Threats	Attacks	Remarks
1	Ensuring Compliance of Law	Strong Virtual Network Framework	Vigilance	Policy Implementation in true letter and spirit	
2	Trusted Platform (TPM)	Virtual Network Framework	VM Security Framework	Policy Implementation in true letter and spirit	• Security is an individual responsibility • Any strong security circle can be breached through individuals
3	Identity Management	FR Techniques	Hyper-safe	Encryption	
4	Antivirus	Hypersafe	VM Detection	Image Management Framework	
5	Virtualization Framework	Trusted Cloud Computing Platform (TCCP)	Disable Memory Duplication	Formal Verification	
6	-	-	Firewalls	Hardware Assisted Solutions	
7	-	-	Encryption and Decryption	-	
8	Identity theft	-	-	Policy Implementation in true letter and spirit	
9	Reasonable Safety against Malware infections and data breaches	-	Security Updates	Policy Implementation in true letter and spirit	
10	Minimizing Customer trust and potential revenue loss	-	-	Policy Implementation in true letter and spirit	

5. CONCLUSION

Virtualization is a very powerful feature provided by the cloud computing paradigm. It allows a person to avail storage, performance, computation resources from distributed servers deployed worldwide. With virtualization, there also lies several security issues that need to be addressed to provide the consumers with a safe and secure environment. We have done an extensive survey of the literature to find out different ways by which virtualization could be achieved in a cloud computing environment. Furthermore, we have also analyzed the literature to find out different types of threat, attacks that could be made on a virtual machine. Various security challenges and issues have also been included in this survey report. Various security frameworks have also been discussed in this report that promise to ensure security in virtualized cloud environments. For the ease of readers, we have categorized the data collected from literature and exhibited it in the form of matrix. This report tends to provide the researchers with an opportunity to learn about virtualization, techniques of virtualization in cloud environments, the challenges and issues faced by cloud engineers to make the virtualization secure in cloud computing. We will be adding more details into this survey report as new literature is published and with the passage of time the challenges emerge in this domain. Virtualization provides us with storage, performance, computation resources from distributed servers deployed worldwide. With virtualization, there also lies several security issues that need to be addressed to provide the consumers with a safe and secure environment. We have done an extensive survey of the literature to find out different ways by which virtualization could be achieved in a cloud computing environment. Furthermore, we have also analyzed the literature to find out different types of threat, attacks that could be made on a virtual machine. Various security challenges and issues have also been included in this survey report. Various security frameworks have also been discussed in this report that promise to ensure security in virtualized cloud environments.

REFERENCES

[1] Jin, Hai, Aaqif Afzaal Abbasi, and Song Wu. "Pathfinder: Application-aware distributed path computation in clouds." International Journal of Parallel Programming 45, no. 6 (2017): 1273-1284.

[2] Cloud Computing Characteristics and Services: A Brief Review Aaqib Rashid1 IJCSE, 2019

[3] Abbasi, Aaqif Afzaal, Hai Jin, and Song Wu. "A software-defined cloud resource management framework." In Asia-Pacific Services Computing Conference, pp. 61-75. Springer, Cham, 2015.

[4] Nalini Subramanian et al. "Recent security challenges in cloud computing" ELSIEVER, 2018.

[5] , "A Study on the Research Challenges and Trends of Cloud Computing"Yeshwanth Rao Bhandayker,JRR,2019.

[6] Research gaps based virtualization in mobile cloud computing Boubakeur Annane1 2020.

[7] Manish Kumar Abhishek et al. Containerized Placement of High-Performance Computing in Cloud, 2019 .

[8] Mohammad Haris et al. A Systematic Review on Cloud Computing, 2019.

[9] Julia Siderska et al, Cloud manufacturing: a service-oriented manufacturing paradigm. A review paper, 2018.

[10] Theodor Borangiu et al. Digital transformation of manufacturing through cloud services and resource virtualization, 2018.

[11] Abbasi, Aaqif Afzaal, Sameen Javed, and Shahaboddin Shamshirband. "An intelligent memory caching architecture for data-intensive multimedia applications." Multimedia Tools and Applications (2020): 1-19.

[12] Batool, Faiza Eba, Muhammad Attique, Muhammad Sharif, Kashif Javed, Muhammad Nazir, Aaqif Afzaal Abbasi, Zeshan Iqbal, and Naveed Riaz. "Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM." Multimedia Tools and Applications (2020): 1-20.

[13] Blesson Varghese et al. Next generation cloud computing: New trends and research directions, 2017.

[14] Jenia Afrin Jeba et al. Towards Green Cloud Computing an Algorithmic Approach for Energy Minimization in Cloud Data Centers, 2019.

[15] Pal, A. Souvik, and B. Prasant Kumar Pattnaik. ”Classification of virtualization environment for cloud computing.” Indian Journal of Science and Technology 6.1 (2013): 3965-3971.

[16] Liu, Yihe, Aaqif Afzaal Abbasi, Atefeh Aghaei, Almas Abbasi, Amir Mosavi, Shahab Shamshirband, and Mohammed AA Al-qaness. "A Mobile Cloud-Based eHealth Scheme." arXiv preprint arXiv:2004.11842 (2020).

[17] Abbasi, Aaqif Afzaal, Shahab Shamshirband, Mohammed AA Al-qaness, Almas Abbasi, Nashat T. AL-Jallad, and Amir Mosavi. "Resource-Aware Network Topology Management Framework." arXiv preprint arXiv:2003.00860 (2020).

[18]Shukur, Hanan, et al. ”Cloud computing virtualization of resources allocation for distributed systems.” Journal of Applied Science and Technology Trends 1.3 (2020): 98-105..

[19] Sabahi, Farzad. ”Secure virtualization for cloud environment using hypervisor-based technology.” International Journal of Machine Learning and Computing 2.1 (2012): 39..

[20] Vaezi, Mojtaba, and Ying Zhang. ”Virtualization and cloud computing.” Cloud Mobile Networks. Springer, Cham, 2017. 11-31.

[21] Xing, Yuping, and Yongzhao Zhan. ”Virtualization and cloud computing.”Future Wireless Networks and Information Systems. Springer,Berlin, Heidelberg, 2012. 305-312..

[22] Kazim, Muhammad, et al. ”Security aspects of virtualization in cloud computing.” IFIP International Conference on Computer Information Systems and Industrial Management. Springer, Berlin, Heidelberg, 2013..

[23] Hashizume, Keiko, et al. ”An analysis of security issues for cloud computing.” Journal of internet services and applications 4.1 (2013):5..

[24] Nagesh, O., Tapas Kumar, and Vedula Venkateswararao. ”A Survey on Security Aspects of Server Virtualization in Cloud Computing.” International Journal of Electrical and Computer Engineering (2088- 8708) 7.3 (2017)..

[25] Ahmad, Naim. ”Cloud computing: Technology, security issues and solutions.” 2017 2nd International Conference on Anti-Cyber Crimes (ICACC). IEEE, 2017.

[26] Mishra, Ankur, et al. ”Cloud computing security.” International Journal on Recent and Innovation Trends in Computing and Communication 1.1 (2013): 36-39..

[27] Luo, Shengmei, et al. ”Virtualization security for cloud computing service.” 2011 International Conference on Cloud and Service Computing. IEEE, 2011..

[28] Asvija, B., R. Eswari, and M. B. Bijoy. ”Security in hardware assisted virtualization for cloud computing—State of the art issues and challenges.” Computer Networks 151 (2019): 68-92. .

[29] Luo, Xiangyang, et al. ”Virtualization security risks and solutions of Cloud Computing via divide-conquer strategy.” 2011 Third International Conference on Multimedia Information Networking and Security. IEEE, 2011. .

[30] Modi, Chirag N., and Kamatchi Acha. ”Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review.” the Journal of Supercomputing 73.3 (2017): 1192-1234..

[31] Malhotra, Lakshay, Devyani Agarwal, and Arunima Jaiswal. ”Virtualization in cloud computing.” J. Inform. Tech. Softw. Eng 4.2 (2014): 136. .

[32] Gupta, Manjeet, Devesh Kumar Srivastava, and Durg Singh Chauhan. ”Security challenges of virtualization in cloud computing.” Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. 2016..

[33] Sgandurra, Daniele, and Emil Lupu. ”Evolution of attacks, threat models, and solutions for virtualized systems.” ACM Computing Surveys (CSUR) 48.3 (2016): 1-38.

[34] Abbasi, Aaqif Afzaal, and Andreea Florentina. "An Analysis of QoS specific Coherence Issues in Distributed

Networks." International Journal of Advanced Science and Technology 49 (2012): 73-82

[35] Deepika, Tenepalli, and Appini Narayana Rao. ”Active resource provision in cloud computing through virtualization.” 2014 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2014..

[36] Wang, Chu-Fu, Wen-Yi Hung, and Chen-Shun Yang. ”A predictionbased energy conserving resources allocation scheme for cloud computing.”2014 IEEE International Conference on Granular Computing (GrC). IEEE, 2014. .

[37] Kruekaew, B., and W. Kimpan. ”Virtual machine scheduling management on cloud computing using artificial bee colony.” Proceedings of the International MultiConference of engineers and computer scientists. Vol. 1. 2014. .

[38] Student, U. G. ”Dynamic resource allocation scheme in cloud computing.” Procedia Computer Science 47 (2015): 30-36..

[39] Pradhan, Pandaba, Prafulla Ku Behera, and B. N. B. Ray. ”Modified round robin algorithm for resource allocation in cloud computing.” Procedia Computer Science 85 (2016): 878-890..

[40] Padmavathi, M., and Shaik Mahaboob Basha. ”Dynamic and elasticity ACO load balancing algorithm for cloud computing.” 2017 International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2017.

[41] Abbasi, Aaqif Afzaal, Mohammed AA Al-qaness, Mohamed Abd Elaziz, Ammar Hawbani, Ahmed A. Ewees, Sameen Javed, and Sunghwan Kim. "Phantom: Towards Vendor-Agnostic Resource Consolidation in Cloud Environments." Electronics 8, no. 10 (2019): 1183.

[42] Abbasi, Aaqif Afzaal, Mohammed AA Al-qaness, Mohamed Abd Elaziz, Hassan A. Khalil, and Sunghwan Kim. "Bouncer: A Resource-Aware Admission Control Scheme for Cloud Services." Electronics 8, no. 9 (2019): 928.

[43] Usman, Mohammed Joda, et al. ”Energy-Efficient virtual machine allocation technique using interior search algorithm for cloud datacenter.” 2017 6th ICT International Student Project Conference (ICT-ISPC). IEEE, 2017..

[44] Akintoye, Samson B., and Antoine Bagula. ”Optimization of virtual resources allocation in cloud computing environment.” 2017 IEEE AFRICON. IEEE, 2017.

[45] Atiewi, Saleh, Abdullah Abuhussein, and Mohammad Abu Saleh. ”Impact of Virtualization on Cloud Computing Energy Consumption: Empirical Study.” Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control. 2018.

[46] Yin, Shuang, Peng Ke, and Ling Tao. ”An improved genetic algorithm for task scheduling in cloud computing.” 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE, 2018.

[47] Chen, Jing. ”A cloud resource allocation method supporting sudden and urgent demands” 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD). IEEE, 2018.

[48] Rengasamy, R., and M. Chidambaram. ”A Novel Predictive Resource Allocation Framework for Cloud Computing.” 2019 5th InternationalConference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2019.

[49] Khodar, Almothana, Hazim Abdulameer Fadhil Al-Afare, and Iyad Alkhayat. ”New Scheduling Approach for Virtual Machine Resources in Cloud Computing Based on Genetic Algorithm.” 2019 International Russian Automation Conference (RusAutoCon). IEEE, 2019.

[50] Beres, Remus Narcis, et al. ”A review of passive power filters for three-phase grid-connected voltage-source converters.” IEEE Journal of Emerging and Selected Topics in Power Electronics 4.1 (2015): 54-69. .

[52] Wu, Ziran, et al. ”A traveling-wave forward coupler design for a new accelerating mode in a silicon woodpile accelerator.” IEEE Journal of Selected Topics in Quantum Electronics 22.2 (2015): 162-170. .

[52] Jin, Seongwook, et al. ”H-SVM: Hardware-assisted secure virtual machines under a vulnerable hypervisor.” IEEE Transactions on Computers 64.10 (2015): 2833-2846.

[53] Abbasi, Aaqif Afzaal, and Mureed Hussain. "A QoS enhancement framework for ubiquitous network environments." International Journal of Advanced Science and Technology 43 (2012): 37-48.

[54] Liang, Hongliang, et al. ”A lightweight security isolation approach for virtual machines deployment.” International Conference on Information Security and Cryptology. Springer, Cham, 2014.

\end{document}