Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Secure mitigation and migration of virtual machines over hybrid cloud hypervisors infrastructure

Badr Almutairi *

Department of Information Technology, College of Computer Sciences and Information Technology, Majmaah University, Al-Majmaah, Saudi Arabia

ARTICLE INFO

Article history:
Received 23 October 2020
Received in revised form
9 January 2021
Accepted 6 February 2021

Keywords:
Virtualization
Hypervisors
Virtual machines
Mitigation
Migration

ABSTRACT

As workloads increase in the industry so does the requirement for IT resources. IT companies are now shifting from in-house data centers to cloud-based IT services such as IAAS, PAAS, and SAAS which can offer flexibility at different levels to the developers of the applications working on different projects. Lots of researchers have contributed to migrating virtual machines migration from one cloud service provider to the other in case of backup as a service and other related services. Some of the previous works by some researchers focus on the migration of SAAS and PAAS onto different cloud service provider platforms. This research work focuses on the mitigation and migration of IAAS, PAAS, and SAAS services of the cloud. My contribution in this research will be in how to avoid loss of data during mitigation and migration of the VM from one Hypervisor environment to the other hypervisor environment on a physical machine infrastructure. This will help SME's to provide end-user access to their data without worrying about the losses which may have incurred if the Mitigation process was not carried out carefully while migrating VM's from one bare metal Hypervisor environment to the other bare metal Hypervisor environment.

1. Introduction

Cloud Computing is being used in large data centers and cloud service providers are providing accessibility, availability, and reliability for the virtual machines which are being created by the customers on the cloud data center all these serveries are being monitored using a remote administration system the QoS (quality of service) agreement which is signed along with the SLA's (service level agreement) by the customer is important as this grantees the customer that the cloud service provider will give all the services and availability of the services 24x7. The cloud service provider has deployed large physical data centers (PDC). These large data center's host lots of physical machines on which the virtualization environments are configured and running 24x7 it's also important for the cloud service provider to provide backup solutions in case of the failover of physical infrastructure and zero downtime to the end-user or customer as it may be written in their SLA's (Choudhary, 2016a). As virtual machines created by the customers are running 24x7 to cater to their end-users with the services which the companies are offering it's important for the cloud service providers to keep track of the uptime and service availability of the customers if the physical infrastructure is down due to any reason it's the job of the cloud service provider to give redundancy for the infrastructure which is running critical applications of the customer so that the end-users do not face any downtime. As virtual machines created by the customers run real-time critical services which are serving millions of end-users around the cloud in different locations it's important to keep replication of virtual machines and the data should be protected from attackers and viruses. Replication of virtual machines will also help the cloud service providers to provide instant backup service along with the client's data. As the IT infrastructure required to the application online without managing them is really pleasing but the risk associated with it is to be considered when deploying real-time critical applications on the cloud infrastructure. Security is one of the most important concerns for the customers when using cloud IT infrastructure as the physical IT resources are governed by privacy and

* Corresponding Author.
Email Address: b.algoian@mu.edu.sa

https://doi.org/10.21833/ijaas.2021.07.002
Corresponding author's ORCID profile:
https://orcid.org/0000-0003-1187-6908
2313-626X/© 2021 The Authors. Published by IASE.

security law in the country of IT infrastructure deployment. Virtualization provides IT resource availability at less cost and time but it comes with big concern about security. As security is one of the major concerns for many companies using the cloud to deploy their applications online in an untrusted environment. As most of the cloud services providers are guaranteeing that they are secure IT infrastructure providers but the gain of the consumers' concern is a big challenge in the cloud computing industry even today (Lawal and Nuray, 2018). As IT infrastructure requested by the customer is provisioned on the cloud service provider's end with minimum interaction all IT resources are being released online with less interaction on the cloud service provider's end. As the virtualization technique helps in separating the physical infrastructure from the virtual environments it provides an underlying layer that protects the user's data and the operating system on which the applications are running. The customer does not need to worry about physical infrastructure provisioning in case of increased traffic to the application or the services which he is providing as the IT resources can be scaled easily in the cloud infrastructure. As multiple virtual machines can reside on one physical infrastructure it's important for the cloud service provider to isolate them from each other despite they may be sharing the same physical space in the data center on which they have been created. This will protect the integrity of end user's data on the cloud data center. As the virtual machines are software versions of the physical IT infrastructures their size may also vary based on the data which is being carried by the application which is running on them. A hypervisor is a software solution that helps in creating a virtualization layer on top of the physical infrastructure which helps the cloud service provider to scale the IT resources which are required by the cloud consumer at any time based on workload which may increase indifferent geographic location where the services are running. As cloud computing models are used for delivering flexibility for on-the-go resource utilization from the pooled resources which are provided by the cloud service provider. Hypervisor solution provides running multiple operating systems on one physical infrastructure with shared IT resources. When multiple VM's are created on a single hypervisor which are sharing multiple IT resources and running multiple operating systems with different workloads at different time periods and located geographically apart it's important to isolate and mitigate the virtual machines from one another so that the risk of losing the data can be avoided and as the virtual IT resources are separate for each virtual machine the possibility of attacking multiple environments at the same time can be avoided. Fig. 1 explains how VM environments are created and deployed on the physical IT infrastructures. Migration of the virtual machines from one physical infrastructure in case of failure on one physical IT resource can be done easily using the hypervisors which have the same configuration on different virtual servers. Physical IT infrastructure over virtualization using hypervisors which are of same configuration help in migration of the virtual machines to provide redundancy in case of failure or security birch on or over the physical network this helps the customer to keep his services and applications running 24x7. Data associated with the virtualization storage are also replicated by cloud service providers around different geographical regions so that the availability and throughput of the application utilizing the data can access it easily so that performance of the end customer application increases.

As the requirement for end-user computing is increasing day in and out it's important for the cloud service providers to provide computing services 24X7 to the end-users. As virtual machines run on the physical infrastructure which may be located in different geographical regions it's important to keep the physical infrastructure up and running by the cloud service provider. The IAAS (infrastructure as a service) and PAAS (Platform as a service) are critical components of the cloud which must be provided to the end-user to deploy their services on the virtual machines. As physical data centers for large companies are located geographically apart it's important that the synchronization between these physical infrastructures should be done on time to time basis so that redundancy can be provided by the cloud service providers to the cloud consumers. Mitigation of the virtual machine environments from each other is crucial as attacks and vulnerabilities can be kept away from percolating to shared resources being used by different customers (Choudhary, 2016b). Virtual servers on which multiple virtual machines are running can be pooled and consolidated so that only the required number of servers are up and running with redundancy in different geographical regions. If proper pooling on the virtual servers is carried out, then this will also reduce the carbon print and provide green computing environments for the cloud service providers. As cloud service providers have physical data centers in different regions around the globe data localization can be provided for the customer application which will improve the efficiency of the application usage and provide a performance boost to the consumer of the cloud. As the demand for IT resources for VM's keep changing and to keep resource availability for the VM's running important applications of the customer. The cloud service provider keeps on migrating the VM's over the physical infrastructure to keep all services up and running as requested by the customers this an overhead for the cloud service provider as he needs to keep all IT resources up and running 24x7 so that failovers and live migrations can be achieved in case of request of IT resources by the customer.

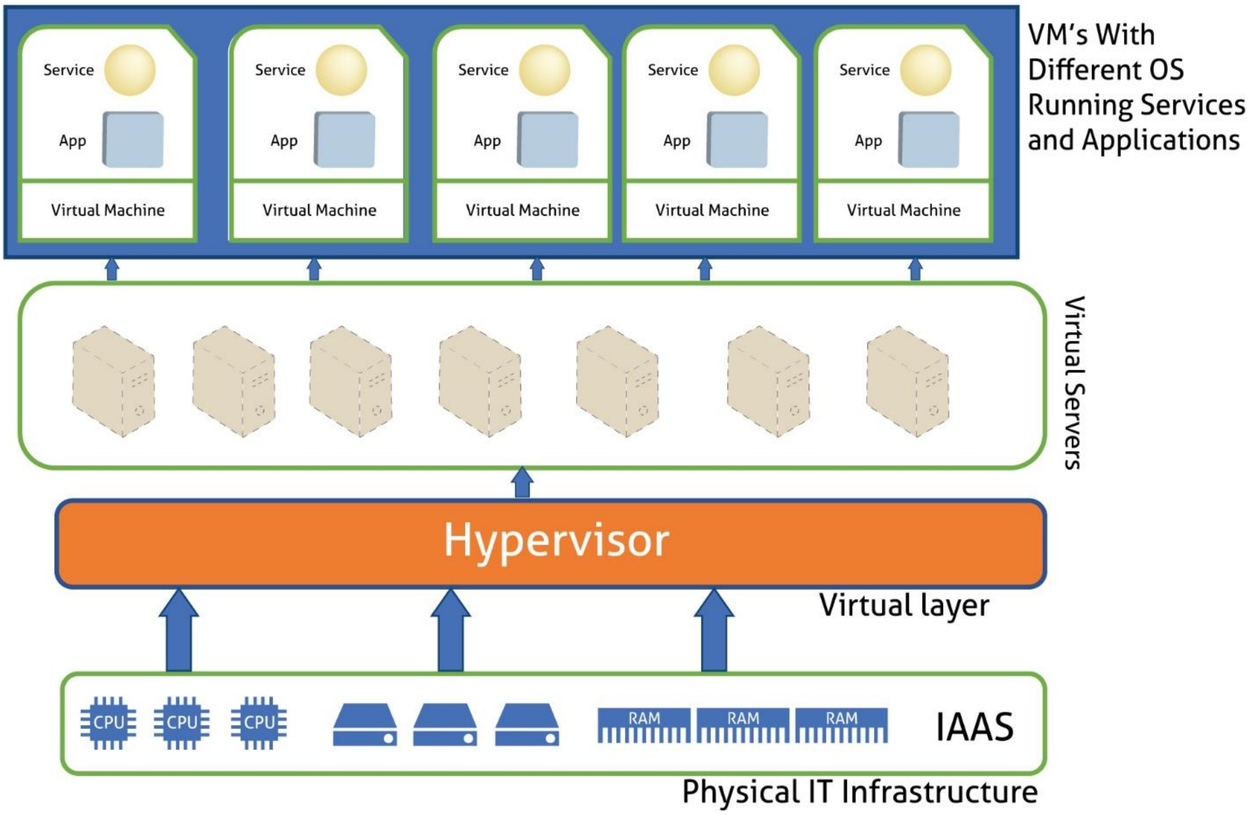

Service
App
Virtual Machine
VM's With Different OS Running Services and Applications
Virtual Servers
Hypervisor
Virtual layer
CPU
RAM
IAAS
Physical IT Infrastructure

Fig. 1: Cloud computing environment

2. Literature review

In this research work, literature has been collected from various sources like printed journals, magazines, and online resources some of the research works have been briefly described below.

Survey on mitigation techniques of virtualization technique in this research work the author would like to focus on how cloud computing is a boom to the industry but along with all resource flexibility, scalability, and IT resource availability, the major problem which is found in the cloud computing industry today is security which is a key factor concerning the cloud consumers. The researcher provides techniques that can help in mitigating and avoiding vulnerabilities to attack at different levels of the cloud computing environment (Usmani and Singh, 2016). One of the techniques which the author explains is hyper-jacking which helps in protecting the hypervisors from getting attached by the hackers. Also, the author explains the denial of service mitigation technique which helps the cloud service providers to protect their machines and IPs from getting attacked with Dos (Denial of service attack).

A survey of virtual machine placement techniques in a data center in this research article the author explains how server consolidation can help green computing for the cloud service providers but also focuses on the availability of resource during peak hours how VM's can be placed and migrated to the physical environment on-demand based on customer requirements. How to overcome the demand and scalability of VM's (Usmani and Singh, 2016). The host load calculation should be done for consolidation of servers if its found that hosts are under loaded then migration of the VM's can be done from one host to the other but this migration of the VM should be performed live so that the customer services are not affected and the data stays intact. Load balancing of the virtual servers should be done so that after migration of the VM's the efficiency of the customer should not be degraded.

A Critical Analysis of Energy Efficient Virtual Machine Placement Techniques and its Optimization in a Cloud Computing Environment in this research article the author explains how optimization of virtual machines can be done with live migration to running virtual servers so that the servers can be utilized with efficiency and effectively using dynamic thresholding technique live migration of the virtual machines can be done which will reduce the carbon footprints of cloud service providers. As pooled IT resources can be up and running with minimal downtime if optimization is achieved at different levels of cloud computing environments (Huseynov et al., 2020). VM's can be classified based on the power utilization and application utilization that is running on the live VM's also migration can be done to fulfill the optimum utilization of IT resources of the IT infrastructure.

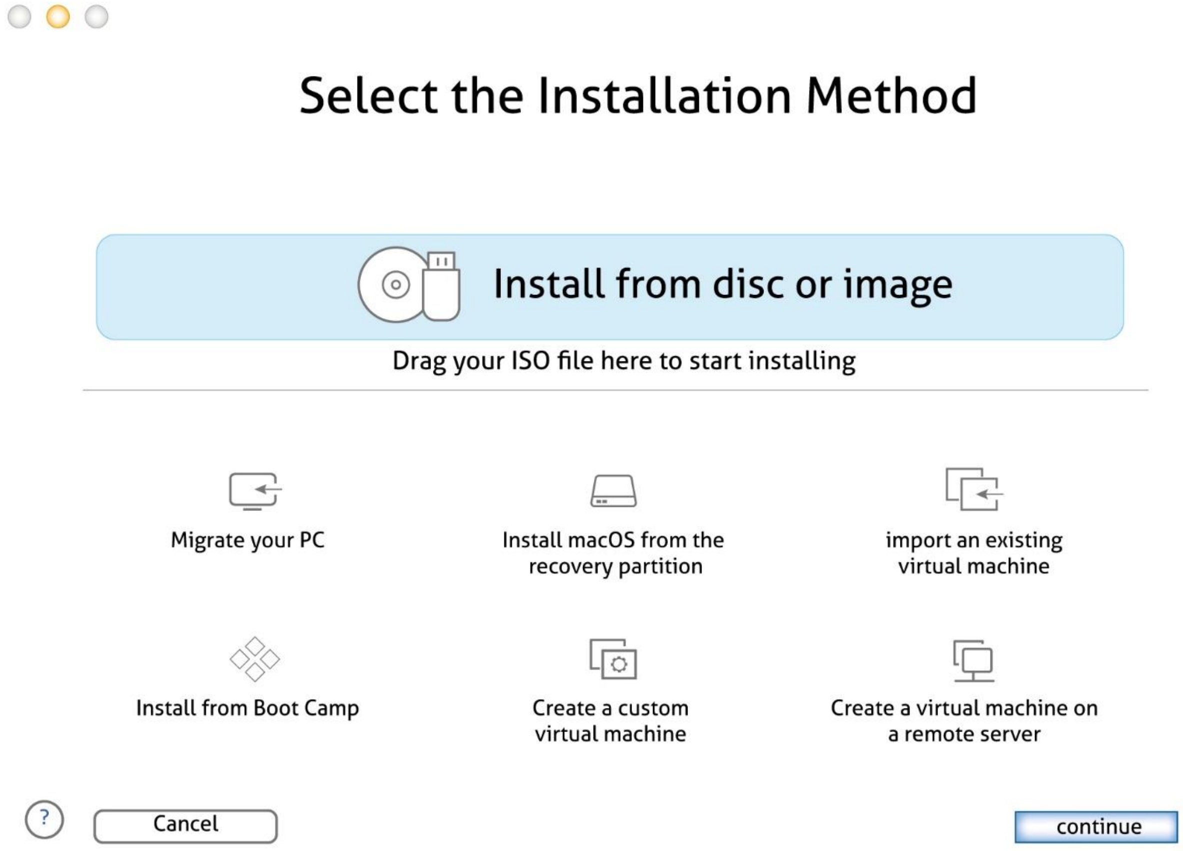
Virtual Machine Migration Triggering using Application Workload Prediction in this research article the author would like to focus on the dynamic provisioning of physical IT resources. This can be achieved using the vertical scaling live migration can be performed so that the performance and utilization of the physical resource can be done efficiently (Raghunath and Annappa, 2015). Triggers can be prepared for migration of the virtual machines based on the workload which is monitored by the virtual machines running the applications if less workload is found then migration of lower IT resources can be done and other resources can be on standby when the workload increases then more performance-oriented IT resources can be provided to the VM's running customer applications.

3. Secure mitigation of cloud computing environment

As cloud computing provides massive IT resources as scalability at large which brings lots of SME's and large scale companies to use rich IT infrastructure at less cost and the OPEX (Operational Expenditure) to manage and maintain the infrastructure is zero which helps in utilizing this amount in some other operations of the company also the Capital expenditures (CAPEX) which are companies long term expenditure are also reduced to achieve a reduction in all of these operational expenditures the companies SME's and the large scale industries move to cloud computing IAAS, PAAS and SAAS services which are provided the cloud companies. But the major challenge in moving from the current IT infrastructure to the cloud needs provisioning or the resources software and hardware which will help in deploying the customer applications successfully online onto the cloud infrastructure on which the company has decided to host its services. This process requires mitigation of the resources and services which are currently running on the customers' data center to be migrated to the virtualization environment successfully without any downtime while the customers may be connected to important services which service provider is providing to the end-users. Following services are provided to the consumer of the cloud:

1. PC Migration service
2. Improve Existing Virtual Machines
3. Create a custom virtual machine
4. Create a virtual machine on a remote server

Fig. 2 shows methods for VM installation.



Select the Installation Method

Drag your ISO file here to start installing

Install from disc or image
Migrate your PC
Install macOS from the recovery partition
import an existing virtual machine
Install from Boot Camp
Create a custom virtual machine
Create a virtual machine on a remote server
?
Cancel
continue

Fig. 2: Methods for VM installation

These services are provided to the end customer by the service provider so that he can securely mitigate his current infrastructure and isolate service dependency so that when the migration of the current software services are done the end-user using the services will not be affected and the migration from the customers' data center to the cloud computing service providers infrastructure will be performed without any downtime in the consumers end. Following mitigation techniques can be used as listed below (Singh et al., 2015). Mitigation techniques can be used as listed below:

1. Avoidance: This technique is used when the migration of the VM's are done from one hypervisor to the other and if the risk is present while migrating the VM's then a rollback of the VM's can be done to avoid any risk associated with the migration process. This not only saves time but also reduces the cumbersome work of rechecking the correct migration of the VM's is done or not. The other process is that this Avoidance technique provides foresee the problems which may occur during the migration process of the VM's thus avoiding the problem which may occur during the VM migration. This technique also helps in testing the VM migration process and checking if the migration process will be executed successfully on the other hypervisor with the same IAAS. Thus, preventing any downtime for the services which are running in the current VM.
2. Acceptance: In this technique, the risk associated while mitigating the machine is less and the chances of failure of mitigation are under acceptable circumstances then the processes of mitigation can be done. If a minor risk is associated which can be overcome at a later stage of mitigation then it's under acceptance to mitigate and migrate the virtual machines.
3. Reduction or Control: Reduction of the risks associate with mitigation of VM's can be done by prioritizing the risk which is likely to occur during the mitigation process and checking the severity of the risk and then handling the risk to avoid any catastrophic failure during the mitigation process this will help in controlling the features and functions of the system during the mitigation process the control can be applied as to protect the occurrence of the large damage to the virtual machine during the VM mitigation process.
4. Transference: While mitigation of the VM's the problem that arises due to a third-party application can be shifted to third parties handling the process of fixing applications and providing bug fix during the VM mitigation process this will reduce the burden of the customer of the cloud to securely mitigate his services without worrying about the third-parties applications which may be causing the failure for the mitigation process of the VM's this will also help in secure mitigation (Hidayat and Alaydrus, 2019).

4. Secure migration of virtual machine in a hybrid environment

As an organization is shifting some applications and services to the cloud computing infrastructure it's important for the customer to decide upon which services are important and are in need of high computing and storage resources that can be securely migrated to the cloud providers platforms which need to be created before carrying out the migration process of the VM's which may be running these services there are few steps which need to be followed by the consumer who is migrating the VM's from his local data center to the cloud providers data center (Kang and Yu, 2018).

4.1. VM compatibility

It's important for the cloud consumer to check which VM's are running application which needs more IT resources and can be migrated to cloud service providers environment before starting the process of migration over the hybrid cloud the cloud consumer needs to segregate the VM's internally on the on-premises data center where he can have a clear idea about which services need to be moved to VM's which need to be migrated (Zhang et al., 2012). Services that are in high demand of IT resources can be shifted to other VM's which are scheduled to be migrated to the cloud providers infrastructure. On the other end, the consumer of the cloud will create VM's with custom specification and same configuration as the VM's which need to be migrated this will reduce the time which is required by the VM's to be migrated to the new infrastructure as both the new and the old IAAS and PAAS will be same so the services which are running will not take much time to go live. Fig. 3 shows secure migration of VM.

4.2. VM shutdown and migration procedure

This process is used when the downtime of the existing VM's will not affect the functioning of the company this is also known as secure migration as there is less risk associated with this type of migration. Here the consumer will shut down the VM's which need to be migrated to the cloud service providers infrastructure once the migration process is completed then the VM's can be started and the services which were running in the VM's can be restarted ad be consumed by the end-user without any issue.

4.3. Live VM migration onto cloud service providers Infrastructure

In this migration process which is having high risk due to services that may be critical for the business are running on the VM's these services should not be shut down as they are being consumed by the end-users. The process of live migration of the VM's is generally carried out during an off-time when the load on the VM's is low which needs to be migrated (Lawal and Nuray, 2018). During the live migration process, the VM's are kept running and all the services are running inside the container VM's the IT infrastructure and the hypervisor versions of the new VM are the same as the migration VM so that there is no delay on the migration of the VM and the process is carried out successfully without any glitch in the migration process. Thus, it's important that the hypervisor versions and the configurations of the client and the service provider of the cloud need to be the same. Fig. 4 shows the live migration of VM.

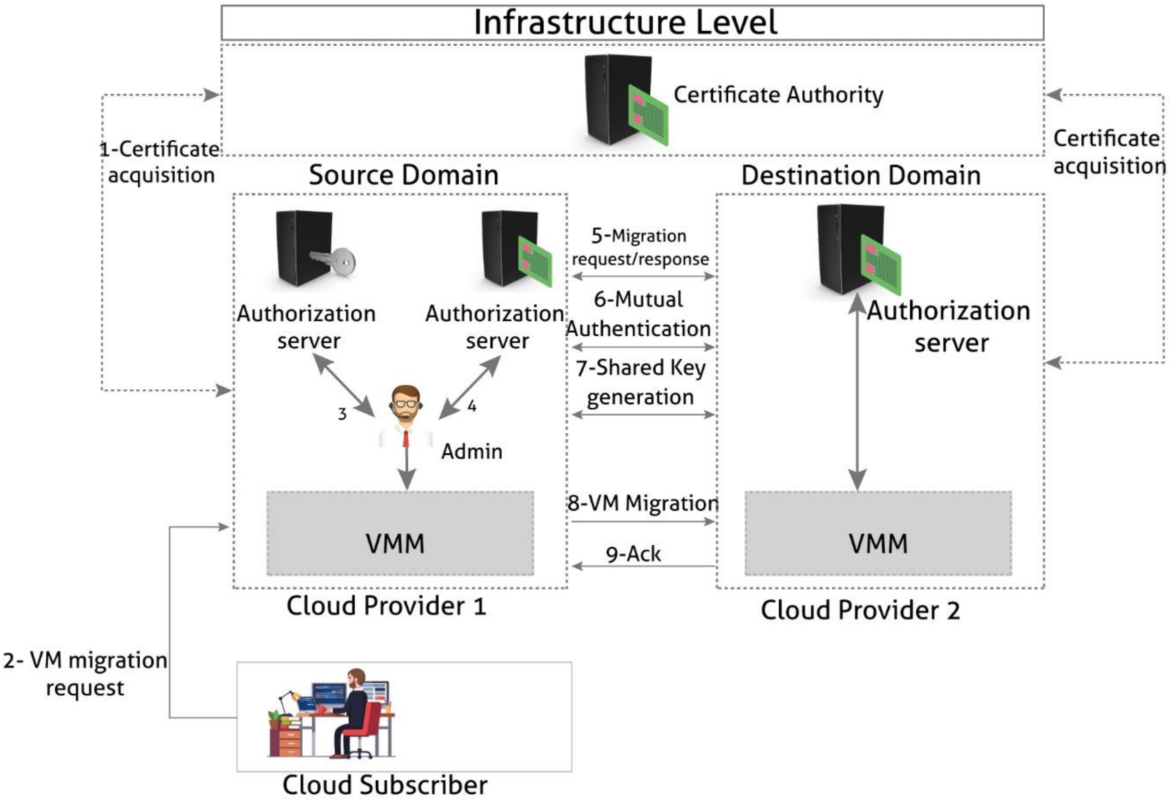


Fig. 3: Secure migration of VM

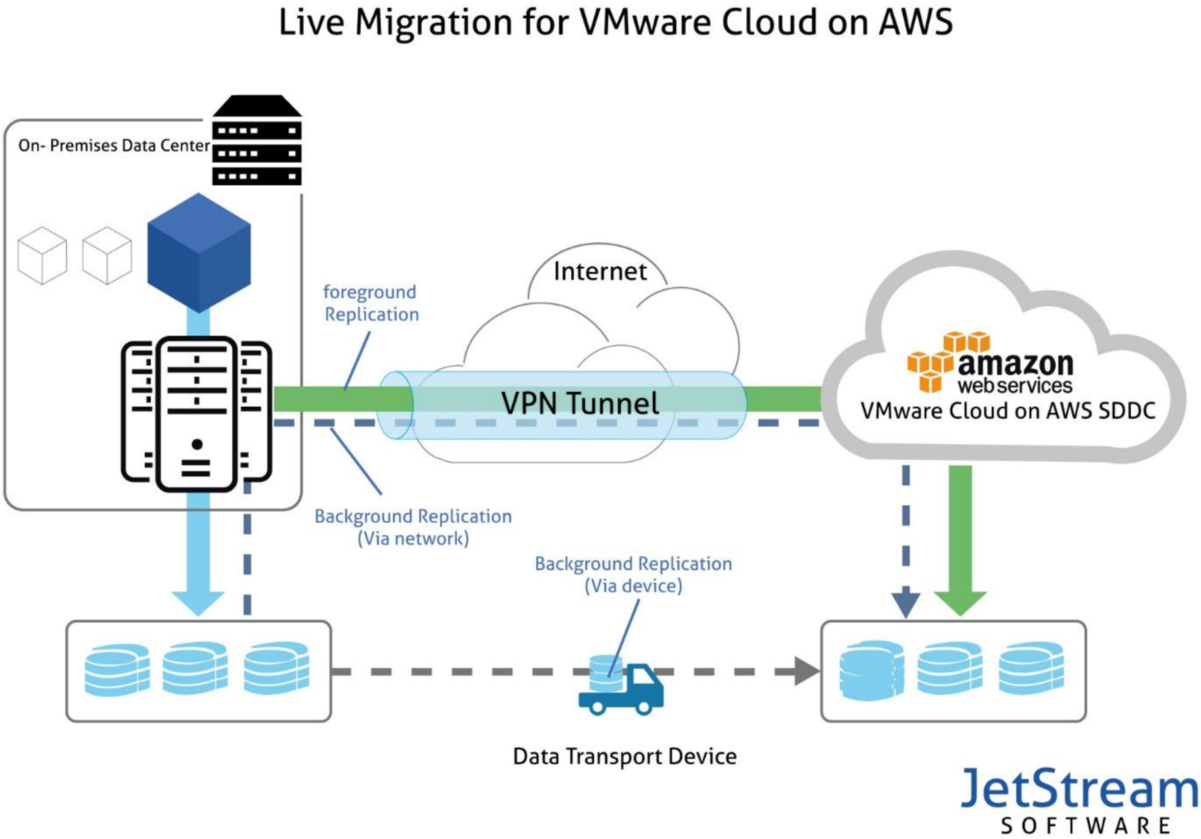


Fig. 4: Live migration of VM

5. Results and discussion

This research work will help in securely mitigating the hypervisor environment for virtual machines which will provide end-user or the consumer of the cloud to migrating virtual machines over different hypervisors. Mitigation of the virtual machine is important as in case one of the virtual machines in the network or on the hypervisor is attacked with any malicious software or by virus then due to the mitigation policies and strategies it will be isolated from the existing hypervisor network and will not affect any other virtual machine running on the same hypervisor environment. When compared with other research work accomplished in this research area it's evident that live migration with mitigation and optimization of VM's will securely migrate machines from one cloud service provider to the other. Thus, by mitigation of VM's over the hypervisors it provides security and integrity for the VM's to be isolated and not affect the other even though they share the common hypervisor environment. In the migration process we need to optimize the migration as discussed above we need to reduce the image size by mitigation and compression of the items which reside inside the VM by doing so we can optimize the virtual machine migration.

6. Conclusion

As virtualization and cloud computing provide scalability of IT resources which come a less CAPEX and OPEX also providing the customer more flexibility for managing and maintaining his virtual machines online. But with all of these flexibilities of IT resource scalability and other services provided by the cloud service providers the major problem which is challenging for IT companies today is security which can be overcome if the mitigation processes are carried out carefully the procedures and policies for mitigation are given in steps which can be followed while mitigating and migrating VM from one hypervisor to the other also the isolation of the hypervisors and the virtual machines is important as exposures of seamless connectivity between virtual machines can create attacks on one another and then bring down the services and the VM which are running also digital certificate should be signed between the end-user of the cloud and the cloud provider so that security can be maintained between two parties who are using and sharing the cloud IT resources. This research paper provides a different method of creation and migration of virtual machines and how they can be achieved with secure mitigation and migration of VM's from one hypervisor to the other in the hybrid cloud computing environment. It also focuses on the migration steps of the VM from one hypervisor to the other with live migration which can be achieved without shutting down any services of the clients. Security is one of the major concerns while migration of the VM but by using mitigation your VM can be secured first and then migrated to the other hypervisor.

Acknowledgment

I would like to thank my university and college for guiding me in the right direction and to keep motivating me for completing this research work. This research work would not have been complete with the core references which have enlighten my knowledge about cloud computing IT infrastructure resources and how they have been playing important role in many industries for enhancing the ever-increasing demand of IT resources by the customer and developers.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Choudhary A, Govil MC, Singh G, Awasthi LK, Pilli ES, and Kumar N (2016a). Improved virtual machine migration approaches in cloud environment. In the IEEE International Conference on Cloud Computing in Emerging Markets, IEEE, Bangalore, India: 17-24. https://doi.org/10.1109/CCEM.2016.013

Choudhary A, Rana S, and Matahai KJ (2016b). A critical analysis of energy efficient virtual machine placement techniques and its optimization in a cloud computing environment. Procedia Computer Science, 78(C): 132-138. https://doi.org/10.1016/j.procs.2016.02.022

Hidayat T and Alaydrus M (2019). Performance analysis and mitigation of virtual machine server by using naive bayes classification. In the 4th International Conference on Informatics and Computing, IEEE, Semarang, Indonesia: 1-5. https://doi.org/10.1109/ICIC47613.2019.8985932

Huseynov H, Kourai K, Saadawi T, and Igbe O (2020). Virtual machine introspection for anomaly-based keylogger detection. In the 21st International Conference on High Performance Switching and Routing, IEEE, Newark, USA: 1-6. https://doi.org/10.1109/HPSR48589.2020.9098980

Kang J and Yu H (2018). Mitigation technique for performance degradation of virtual machine owing to GPU pass-through in fog computing. Journal of Communications and Networks, 20(3): 257-265. https://doi.org/10.1109/JCN.2018.000038

Lawal BH and Nuray AT (2018). Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In the 26th Signal Processing and Communications Applications Conference, IEEE, Izmir, Turkey: 1-4. https://doi.org/10.1109/SIU.2018.8404674 **PMid:31883240**

Raghunath BR and Annappa B (2015). Virtual machine migration triggering using application workload prediction. Procedia Computer Science, 54: 167-176. https://doi.org/10.1016/j.procs.2015.06.019

Singh G, Behal S, and Taneja M (2015). Advanced memory reusing mechanism for virtual machines in cloud computing. Procedia Computer Science, 57(5): 91-103. https://doi.org/10.1016/j.procs.2015.07.373

Usmani Z and Singh S (2016). A survey of virtual machine placement techniques in a cloud data center. Procedia Computer Science, 78: 491-498. https://doi.org/10.1016/j.procs.2016.02.093

Zhang X, Shae ZY, Zheng S, and Jamjoom H (2012). Virtual machine migration in an over-committed cloud. In the IEEE Network Operations and Management Symposium, IEEE, Maui, USA: 196-203. https://doi.org/10.1109/NOMS.2012.6211899