Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

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

Secure PAAS environment over hybrid cloud using load-balanced Docker containers

Ahmad Raza Khan *

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

ARTICLE INFO

Article history:
Received 5 October 2021
Received in revised form
3 January 2022
Accepted 7 January 2022

Keywords:
Docker
Hybrid cloud
Security
Load balancing
Containers

ABSTRACT

The purpose of this research is to provide cloud service providers (CSP) a secure platform that can be accessed for configuring secure, silent software deployment on the hybrid cloud using load-balanced Docker Containers (LBDC) that are configured with different PAAS software solutions. As many researchers in the past have worked on providing PASS platforms using either a public cloud or private cloud less research is carried out on the hybrid cloud systems and researchers who have worked on the hybrid cloud have followed a different approach to providing PAAS to organizations in need but lack in securing the PAAS platform. This research will provide cloud service providers a secure deployment of the PAAS platform for the developers on the go and will reduce the overhead of CSP to deploy the PAAS services from scratch. Compared to the other researcher's contribution this research work provides a load-balanced containerized secure PASS platform that can be scaled on-demand and be secure while scaling the resources for peak workloads. The admins of the hybrid cloud can access and deploy the Docker containers based on the requirement laid down by the developers. Once the Admin configures the Docker container with the required PAAS services he can then easily invoke the LBDC in the hybrid cloud and deploy the PAAS platform for the developers to work on in seconds. LBDC's will help in scalable deployment of Secure PAAS services for different locations and machines simultaneously thus reducing the cost and time required for hybrid virtual machines to get up and running for the development process by the developers of the company. CSP's can achieve less turnaround time for deployment of secure PAAS environments for organizations.

1. Introduction

As cloud provides scalability and availability of resources with zero downtime most large IT organizations are switching to cloud computing for software development and deployment. As the developers are working day in and out for developing large software solutions for organizations around the globe the CSPs are providing more services for companies to reduce the turnaround time from requesting a service to deployment and running the service on their hybrid cloud environments. As platform as a service provides organizations to build more application scalable systems without worrying about the complexities of managing a maintaining large data centers to run software applications PAAS is one such service provided by the CPS which helps in deploying, managing, and maintaining large application software's running large databases and querying data via the application within less possible time by scaling resources of Compute on the go. As many cloud service providers such as AWS, Microsoft, and Google Cloud PAAS platform to a large organization which deploys huge applications software's on the PAAS platforms which can be accessed by the clients from around the globe with zero downtime and high availability. Even today the security issue related to the cloud still haunts the organizations using the PAAS solution provided by the vendors in the market today. As developers are designing an application it's important that the application and the data must be secured when they are deployed at the server end or at the client's premises. Small and Medium Enterprises (SME's) are now shifting their applications to the cloud as the

* Corresponding Author.
Email Address: ar.khan@mu.edu.sa
https://doi.org/10.21833/ijaas.2022.03.015
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-5365-9189

maintenance cost of IT infrastructure on-premises is very expensive and needs lots of resources to the deployed for running the infrastructure (Santikarama and Arman, 2016). As cloud services are easy to provision and deploy it's easy for the application developers and testers can now deploy applications more quickly and test them as soon as the development process is completed. CPSs also provides advanced tools for provisioning servers that can be used directly and are preconfigured with PAAS environments so that once the server is up and running no need to configure third-party applications to run your custom application designed by the company. Data being a critical part of the portal-oriented application integration (POAI) it's important that data of the organization should be hosted on the local IT infrastructure even though the application resides on the cloud PAAS platform.

Hybrid Cloud infrastructure provides more security for data as the data elements can reside on the local IT infrastructure created by the organizations and can be connected to the PAAS environment which is hosting the application. This is providing the organization to secure data on-premise. Dockers Containers provides simplicity of writing applications on the cloud and then migrating these containers based on the load to different servers available. Dockers also provide instant deployment of resources when requested by the applications containers which host the applications can be live migrated from one deployment environment to the other without shutting down the application (Ferrer et al., 2016). Load balancing between the Docker containers can be done by deploying a load-balanced Docker which replicates the deployed application on a new container which then acts as the primary Docker container for the application. Docker containers for different operating systems can be created as many organizations use different software solutions to develop their software solutions Docker can be created based on the organizations' requirements. One of the most prominent technology to create a secure PAAS environment for developers and testers in the company is the Docker containers. This solution of creating PAAS-ready IT infrastructure can be easily crafted as per the development needs of the software programmer and can be deployed for use in seconds which reduces a large task for the IT to find the IT resource for the developer and then provision the resource for deployment purpose. This research will provide a web portal (POIA) that contains various PAAS environments and details of the PAAS services which the PAAS environment will provide to the end-user for deployment at the hybrid cloud infrastructure. Docker containers that are deployed for the PAAS services can be accessed at different levels in the organization and the IT can provision the Docker container which is requested by the developers. Docker uses containers that allow developers to create, run and deploy applications of different PAAS platforms which can be easily configured for development purposes (Tihfon et al., 2016). These containers can then be invoked on the hybrid cloud infrastructure of the organization using different Docker services such as Application program interface (API), Command-line interface (CLI), and Graphical user interface (UI), As Docker containers, are preconfigured by different developers that host different applications and frameworks organization can invoke the container for developers working on different technologies and software design these containers are pre-configured with resources that are required for the project under execution as these container images are secured they can be locally deployed on the hybrid cloud and building applications will become more efficient and quicker for the developers also the overhead of the IT team working round the clock to provide PAAS resources to the development team will also be reduced significantly. Containers are preconfigured and integrated with all favorite tools and technologies which can further be customized if needed for the project. Thus, Docker containers can be customized based on the developer requirements too this will enhance productivity and will reduce the turnaround time for the development of the software in an organization.

Developers can now package and deploy the same instance that they have created for the software development on the client's machine by just replicating the Docker images of the virtual machines as shown in Fig. 1. The system is pre-configured and has all the dependencies for the project to execute at the client premises. The new Docker image can then be hosted on the POAI portal which can then be available for the other developers in the organization. As all the Docker container images are packaged using the Docker libraries they are secure and are having the trust of the trusted contents which are officially downloaded from original vendors of the software applications (Zhao et al., 2019). Docker containers can be shared across organizations and teams for collaborating for the development of the software solution they can also be pushed to the Git Hub repository for public use. All Docker images which are created are published to the Docker hub so when IT administrators access the repository of Docker images they get information about which Dockers were created and who in the organization has created this Docker image and what PAAS platforms are available on the Docker image this will help the administrators to easily commission the Docker image for future use for any project in the organization or for backing up data in the Docker container. As the number of Docker containers increase in the organization it's important to keep track of the containers and the applications which can be hosted using these Docker containers here is where the POAI comes handy by adding all Docker container images information to the repository so that its easily searchable from the POAI portal. Containers that host developer codes can also be provided role-based access so that each user can access certain applications inside the Docker container thus improving the security of the Docker

image. Administrators or project managers can get an insight view of the containers running applications and also the activity history of the Docker container to check the usage of the container image and the security policies associated with the Docker image. Furthermore, audit logs can be maintained for accessibility of the Docker images across the organization thus protecting the usage and access to the container images. LBCD's can be used for large software projects which need more resources and large teams working on different modules inside the project which need different PAAS platforms which need to be running simultaneously so that the development of the client applications can be completed on time and with all resources allocated to the project. These LBCD's will balance load among different container images so that all resources of the containers are not exhausted and can be used for processing clients' requests during peak hours of software utilization (Matthias and Kane, 2015).

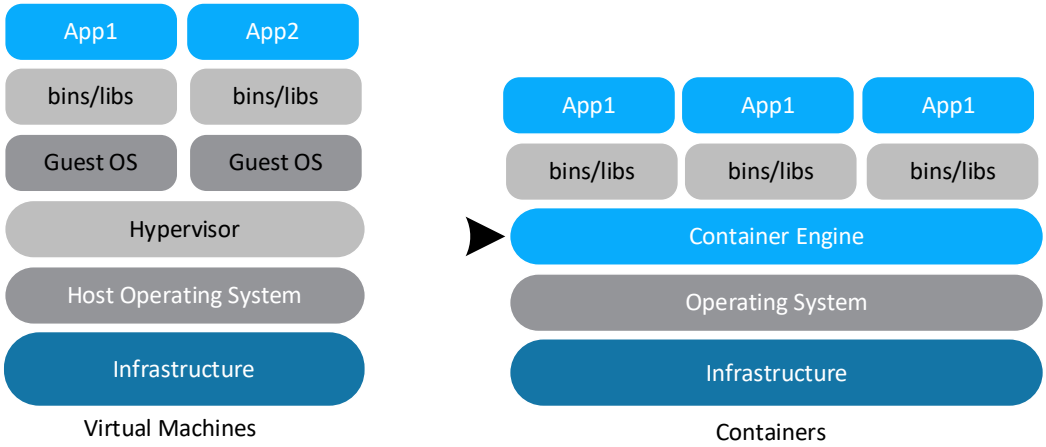

Fig. 1: Virtual machines and Docker containers

2. Literature review

This research work's literature has been gathered from different sources some of them include conferences, journals, white papers, research magazines, and online resource materials here I would like to give an overview of some of the research works.

Bhimani et al. (2016) focused on how the cloud is providing and provisioning resources on the go which can be used for deployment of software applications. Malicious software can be deployed by the vendors of the virtual machines which can further extract critical information and bring down the client's machine without raising any alarms. Side channels can be used to capture information from the deployment servers and VM's and can be given to intruders which overload the system using different attacks and the application will stop running at the clients' end. Co-resident attacks which are deployed on the VM's can be activated by the attackers and information can be sniffed which will then provide insight of the applications and the software which is being deployed on the cloud VM and then the attacker can plan an exact attack which will target the applications which are hosted on the cloud virtual machines. Some of the cloud vendors are also providing dedicated servers which can be used for deployment of the client's applications which are running a side channel or a VM which is hidden on the server once the server is logged on and connected by the client as a remote desktop the attacker VM will fire attacks on the client's machine and sniff information from the machine without the client knowing much about it.

Zhao et al. (2019) emphasized how distributed computing is now stacked on the cloud computing environments with virtualized service solutions. Virtual machines which are created are being overloaded with constant overloads which sometimes creates a problem for the customer running his application on a single virtual machine environment. The author's contribution is to distribute workloads and applications which running on one virtual machine to different Docker swarms which will help in distributed computing of the workload and the software solution deployed on the Docker swarm will remain up even if the load on the application increases due to high application demand by the users. The author also intends to provide the difference between different cloud computing technologies and services which can be used for distributed computing.

Liu et al. (2020) focused on load balancing applications across the computing resources provided by the load balancer which is Kubernetes. This solution provides load balancing at a static level which is not sufficient for large business applications which are running on the cloud thus the author has designed load-balanced Kubernetes which can be used for more efficient workload balance for business applications thus reducing the stress on one machine instance. This solution proposed by the author solves the Kubernetes static load balancing and provides the organization to dynamically load balance loads on different Kubernetes thus reducing the downtime of the application and improving the

throughput of the application too. This solution can be used to dynamically distribute workloads based on the compute information which is captured by the solution which is CPU utilization, bandwidth usage, and disk usage, and reallocate and distribute the load on different virtual machine environments running in the organization.

Orzechowski et al. (2018) explained how different scientific workloads can be distributed over different cloud computing environments without recreating the same environments on different cloud solution providers' cloud infrastructure. Researchers can load their cloud compute environment on central as well as distributed networks which help in hybrid workflow execution of the research work being carried out. Repeating the workflow is protected by the Kubernetes layers on both the central servers as well as the distributed cloud services providers' environment. Research workflows can be executed transparently now on different cloud providers' environments securely. The authors of this research work also provide end-to-end solutions for executing automated workflow environments and managing the lifecycle of the deployment and execution process for the scientific workflows.

Gonzales et al. (2015) illustrated cloud computing software solutions which are provided by different vendors and how they can be trusted and used the solution proposed by the author which is named as Cloud-Trust which provides a quantifiable matrix that can be used the organizations to find the trust levels of the services which the cloud service providers are offering. As cloud computing provides resources for computing on the go it becomes important to access the trust of the services as many vulnerabilities can be found in cloud solutions that can exploit the end-user applications or steal information from the user application which is deployed on the cloud. This system also provides cloud administrators a control system that helps them track the live virtual machines which are running and track the activities of the live virtual machines also the administrators can add more security policies on the virtual machines which are silent or at rest while no operations are being executed to strengthen the virtual machines capabilities to defend the attacks.

Seol et al. (2015) presented the use of hardware and software solutions to protect users' confidential data which can be accessed by administrators due to privilege level and domain controls access. The researchers of this paper have designed custom hardware that can intervein access to the virtual machines if they are not accessed by the authentic users of the machine. This hardware solution proposed will check for the privilege to access the data on a virtual machine and protect the data from being accessed by unauthorized users. This will help in gaining customers' faith in using a virtual machine in the different cloud service providers' environments. The trusted computing base which is proposed will enable securing data and virtual environments from getting attacked or accessed by admins of the same organization due to domain privilege levels.

3. Designing PAAS environments over hybrid cloud

As cloud computing services providers provide PAAS as a service to organizations using different applications it's important to protect end users' data and applications running on the public cloud infrastructures. As the hybrid cloud is the best possible solution for moving organizations to the cloud and building trust on the cloud platforms as it provides flexibility for on-premises IT resources as well as cloud-based services to be connected together to provide one solution for application deployment, design, and testing. To design a platform as a service (PAAS) environment which can be used over the hybrid cloud infrastructure we need to first identify all key stakeholders of the organization and the software platforms which are being used in the organization for development, design, testing, and deployment process for the software solutions. Large organizations have different hierarchies and departments to cater too as the number of user's and employees are located across the globe and have variety of IT resources that are being used in different departments inside the organization. As hybrid cloud provides benefits to the organization for using both on-premises as well as the public cloud infrastructure for scaling on demand by the customer it's important to identify the resources which are being used in different project under execution in the organization. Tools can be used for capturing information of the IT resources such as CPU Utilization, Disk Utilization and much more also information regarding the software's being used for project execution can be captured using tools such as which operating system is being used for development of projects and which software solutions are being used for running applications in the organization. PAAS environment to be deployed on the hybrid cloud needs following key elements to be identified so that the organization can move deployments between public and private infrastructures.

The following points are important for PAAS design:

- Identify software resources being used in the organization
- Collect data about IT resources being consumed by the stakeholders in the organization
- Identify projects which can be hosted on the hybrid cloud
- Identify applications that can be hosted on the hybrid cloud
- Securing data on the hybrid cloud
- Optimization of storage requirements for projects on private and public infrastructure
- Load balancing between the public and private cloud.

As shown in Fig. 2, hybrid cloud PAAS environment has been deployed with Docker containers running packaged applications in the containers which run on the Red Hat Linux environment. The physical infrastructure is hybrid and can be deployed on-demand as the application can scale based on the user's requirement (Ren et al., 2019). As the deployment of the solution is on the Red Hat Linux environment the IT infrastructure is handled by the admin of the organization. A cluster of computing, networking, and security appliances is created on-premises this cluster can be provided for development to the developers on-demand for securing data and critical applications which are catering to high data exchange of the clients as the data need to be secured inside the organization and should not be compromised by the public cloud vulnerabilities.

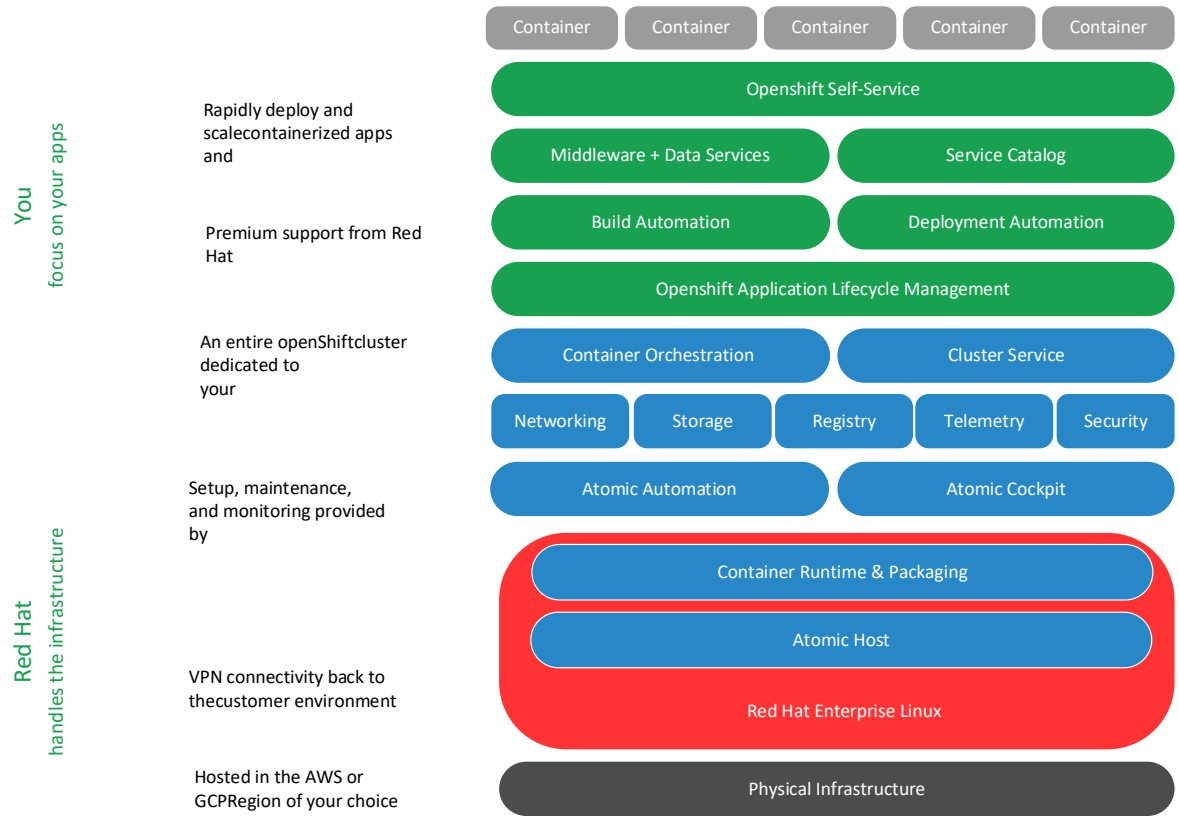

Fig. 2: Design of hybrid cloud for application deployment

The OpenShift container solution is providers lifecycle management of the containers which are running and need to be deployed at the client end the developers of the organization can use this solution to move packaged containers from one virtual environment to the other easily shown in Fig. 2. As all the containers which are running can be packaged with all resources and PAAS services that are running to execute the software solution for the client can be exported as one packaged solution and at the client end, the solution can be deployed without any issues and dependencies.

As shown in Table 1, virtual machines have been created using virtualbox software these virtual machines host the PAAS environment which can be accessed by stakeholders these virtual machines are pre-configured with software's which are requested by different stakeholders using them (Yu et al., 2016). These containers can be moved from one hypervisor environment to the other without a change in configuration and resources. These machines can be used by developers to design applications for clients around the globe testers can use these machines to test applications which are designed by the developers these configurations can also be created on the Docker containers which provide resources available on-demand and shared resources when needed by the development team and other stakeholders using the machines for testing and deployment purpose.

Table 1: Virtual machine containers and resources

Number	VM's Created	Resources Allocated	Operating System Deployed
1	Project Manager 1	CPU i7, Memory 16GB, Storage 100GB	Windows
2	Project Manager 2	CPU i5, Memory 16GB, Storage 200GB	Windows
3	Tester 1	CPU i9, Memory 16GB, Storage 500GB	Linux
4	Tester 2	CPU i5, Memory 8GB, Storage 500GB	Ubuntu
5	Developer Engineer 1	CPU i5, Memory 8GB, Storage 500GB	Fedora
6	Developer Engineer 2	CPU i5, Memory 8GB, Storage 500GB	Arch Linux

4. Creating and running Docker containers with load balancing

Docker containers are instances of PAAS environments that are pre-configured and running online these containers are preconfigured with operating systems and basic software configuration. Containers instances can be deployed in minutes and developers; testers can start working on them immediately. Containers are running as processes on your local machines that are isolated from other processes the container filesystem is isolated from your local machine filesystem hence the local vulnerabilities for your local machine cannot attack the container filesystem (Liu et al., 2010). The filesystem is provided by the image of the container as they are the image of the operating system running with all resources and software solutions including all dependencies that are required to run the application on the clients' end. Administrators can create container images and deploy them on the hybrid cloud so that they can be accessed as an internal resource of the organization. To run a container on the Docker we need to write the following command as shown in Fig. 3.

```
Dr-Ahmad-Raza-Khan: ~ ahmad$ docker run --name Manager -it debian
root@f91okbc9da: # exit
$ docker ps -a | grep Manager
f91okbc9da   debian7    "/bin/bash"   26 second ago   Exited   3 hours ago
```

Fig. 3: Command to run Docker image

The Docker image running on the remote site can be saved on the local server as a zipped file that contains all the PAAS environment dependencies and can be run on the hybrid cloud infrastructure hosted by the organization to save the Docker images on the local deployment servers. To create, start and save a new Docker container you need to run the following commands from the terminal window as shown in Fig. 4.

```
Dr-Ahmad-Raza-Khan: ~ ahmad$ docker create -v /data --name data ubuntu
240633dfbb98128fa77473d3d9019753mdik9c454b3251427ae190a7d951ad57
Dr-Ahmad-Raza-Khan: ~ ahmad$ docker run --rm --volumes-from data ubuntu ls -la
/data
total 8
drwxr-xr-x 2 root root 4096 Dec  5 10:10 .
drwxr-xr-x 48 root root 4096 Dec  5 8:11 ..

Dr-Ahmad-Raza-Khan: ~ ahmad$  docker save myimage:latest | gzip >
myimage_latest.tar.gz
```

Fig. 4: Command to Create run and save a Docker container

To load balance a Docker container to run the same application which can be accessed across different regions within and outside the organization so that the load on the servers in the hybrid cloud is reduced we need to create multiple instances of the container and run those instances on Docker. We can set up an Nginx server that can handle client requests and provide services without the client knowing which server is responding to the request. Using the Nginx server, we can also check for the health of all the servers and how they are performing and balance the load based on the client requests. The filed nodes can be replaced with the new container images to provide zero downtime to the client applications running on the server end. As the container images and the filesystem of the Docker container is different from the local machines its less likely that the attacks which are targeted by the attacker can attack the Docker image instances this way we can protect the data and the applications running on the containers (Goldman et al., 2010). In case of failure of the container running on the hybrid local infrastructure, the load can be balanced by the container running on the public cloud environment hosting the same application this way the end-user will see zero downtime while using the application of the company. Nginx provides high availability by load balancing and running multiple instances of the containers on different cloud services providers instances and also on the hybrid infrastructures.

As shown in Table 2, the percentage of CPU utilization when running a Docker container on the local machine which is running CentOS 7 with PAAS environment and application configured on the system the Average CPU consumed by the system is just 2.5% which is very low as compared to running the application on the local hybrid environment. The average waiting time for the user when accessing the PAAS environment on the container is just 1.0% which is very good as the user will not wait for the CPU response time while accessing the Docker container image shown in Table 3.

Table 2: Percentage of CPU utilization while running instance

Running Instances	Current	Average	Maximum
System	0.1%	2.5%	37.5%
User	1.0%	1.0%	8.6%
Wait	0.1%	35.2%	98.0%
Ideal	98.0%	60.0%	99.0%

Table 3: Percentage of memory utilization while running instance

Running Instances	Current	Average	Maximum
Used	13.0%	53.7%	66.6%
Buffered	0.3%	1.9%	2.0%
Cached	7.7%	38.5%	41.0%
Swap	0.0%	0.0%	1.0%

5. Securing Docker containers and PAAS environments

As Docker containers are pre-configured machines running Linux kernel or windows it becomes important to protect these machines and verify the kernel authenticity. As many users can create a custom container and inject vulnerability in the container images which are then consumed by end-user for running applications online for development and testing proposed. The container which has been created by unknown users needs to be checked before they are run on the hybrid cloud environment. With the ease of use comes more responsibility for the administrators to validate and check the container images before deploying them on the hybrid cloud infrastructure. As containers can be deployed easily and can be accessed across different stakeholders as a shared pool of resources it's more likely that the next image of the container which is created can be vulnerable to attacks if customization is done to the original kernel images deployed by the administrators. To protect the containers from getting attacked it's important that the root access to the container is hidden by the administrator and privilege levels are created to access the container contents. When deploying a container image on the hybrid cloud the administrator needs to create a non-root user so that if any stakeholder requests the container image then he will be granted permission as a user not as a root user to the system even though containers are running as processes attackers can exploit the vulnerabilities in the container image and attack the users root machine hence it's recommended that the administrator should create a user on the system and not deploy container images on the root user. Comparing to the research with other references (Yu et al., 2016; Liu et al., 2010), it has been found that the secure PAAS environment which is created over the hybrid cloud in this research work provides more performance and security as the data which is hosted on the public and the private cloud can now be controlled and that containers can provide more efficiency in running microservices online over the public infrastructures. On the other side load balancing of the containers will provide more network traffic to flow and more users will have access to the PAAS environments with zero downtime other research works show that containers are running as individual units which host microservices of the PAAS environment but if the container fails there is no load balancing provided by the systems thus reliability is a major issue with other research works referenced. This research work provides security, reliability, and zero downtime to PAAS environments and micro stances which are running to server the clients request thus its more effective and efficient system.

Administrators can also create a private registry that can be deployed on the public cloud also this will give full rights to the administrator to deploy container images and manage privilege levels of how container images can be accessed and used across the board. Administrators can also use tools for scanning the container image and check for vulnerabilities if any before deploying the image on the hybrid cloud. Strict control over the Docker container images and who can access them with permission also digital signing of image access can be done. Image authentication and tampering protection rules can be applied in the registry are created. Users from different departments such as development, testing, and production can also be segregated and role-based deployment of container images can be done. Docker images can be kept clean, if the container image is loaded with lots of software platforms then the chances of attack increase the larger the size of the container image the difficult it becomes to manage the image and protect it from attacks. Thus, it is recommended that the container images and kept lightweight so that they can be scanned for vulnerabilities regularly. While pulling a Docker image from the Docker hub or the repository it's important that the image should go under some security checks which is laid down by the administrator of the system once the image is cleared and has been checked then only It can be pulled from the hub to be used by the stakeholders.

As shown in Fig. 5, it's better to pull Docker container images that are of minimal size and then build upon all dependencies which are required to run your application this way you will have full control over the image and will not have to check for any unknown files or software's which may be running on large containers.

6. Results and discussion

Results of this research work show that though Docker containers are easy to deploy and run applications we need to secure them for the PAAS environment. When creating a Docker image with application software running with all dependencies and deploying the image on the hybrid cloud it's important to protect the privacy of the image and also check for vulnerabilities associated with the Docker containers during the deployment process at the clients' end. PAAS environments provided by load-balanced Docker containers reduce the turnaround time for the developers to deliver the

applications to the customers on time as the container images which are provided by the Docker repository as ready to use with all dependencies and can be preconfigured on the client end without worrying about the dependencies of IT resources at the clients end thus reducing the burden of the deployment engineer.

Fig. 5: Compressed size Docker image with minimal Ubuntu version

Container images can be shared across the development lifecycle of the project and be used by different stakeholders involved in the project so that all stakeholders perform their tasks without any issues and errors. Developers, testers, and production units can use the same container images that are configured for the client's PAAS environment and deploy them directly onto the client's infrastructure without any issues in the application running on the container images.

7. Conclusion

I would like to conclude by saying that a secure PAAS environment can be deployed over the hybrid cloud using the load balanced Docker container images which provide more flexibility and ready to use environment for developers, testers, and production engineers to create applications without worrying about the resources scarcity and application depend on abilities which are a key reason for the failure of the project. Thus, by using this method of deployment of PAAS over the hybrid cloud all stakeholders can access an adequate amount of resources for running their projects and also provide more outcomes to the project under execution all stakeholders working the same project can have access to the same Docker image by pulling the image from the central repository and with all dependencies, the image is ready for testing and deployment at the customers end. Docker containers also provide security at different levels so administrators of the organization can configure the Docker images and can also scan the container images before they can be deployed on the end user's system. Docker containers can be load balanced such that applications running on one machine can be replicated with all dependencies on the other container without bringing the first container down thus the application will have zero downtime and the Docker container can be replicated on the go. This will reduce time and load on the single container running the application and will provide load balancing between different container images which are running the same application on different instances of the machine. The resource of the first image will be automatically replicated on the second image with all dependencies that are required to run the program on the second instance.

Acknowledgment

Dr. Ahmad Raza Khan would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2021-278.

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

Bhimani J, Yang J, Yang Z, Mi N, Xu Q, Awasthi M, Pandurangan R, and Balakrishnan V (2016). Understanding performance of I/O intensive containerized applications for NVMe SSDs. In the 35th International Performance Computing and Communications Conference (IPCCC), IEEE, Las Vegas, USA: 1-8. https://doi.org/10.1109/PCCC.2016.7820650

Ferrer AJ, Pérez DG, and González RS (2016). Multi-cloud platform-as-a-service model, functionalities and approaches. Procedia Computer Science, 97: 63-72. https://doi.org/10.1016/j.procs.2016.08.281

Goldman K, Sailer R, Pendarakis D, and Srinivasan D (2010). Scalable integrity monitoring in virtualized environments. In the fifth ACM workshop on Scalable trusted computing, Association for Computing Machinery, Chicago, USA: 73-78. https://doi.org/10.1145/1867635.1867647

Gonzales D, Kaplan JM, Saltzman E, Winkelman Z, and Woods D (2015). Cloud-Trust—A security assessment model for infrastructure as a service (IaaS) clouds. IEEE Transactions on

Cloud Computing, 5(3): 523-536.
https://doi.org/10.1109/TCC.2015.2415794

Liu Q, Haihong E, and Song M (2020). The design of multi-metric load balancer for Kubernetes. In the International Conference on Inventive Computation Technologies (ICICT), IEEE, Coimbatore, India: 1114-1117.
https://doi.org/10.1109/ICICT48043.2020.9112373

Liu Q, Weng C, Li M, and Luo Y (2010). An In-VM measuring framework for increasing virtual machine security in clouds. IEEE Security and Privacy, 8(6): 56-62.
https://doi.org/10.1109/MSP.2010.143

Matthias K and Kane SP (2015). Docker: Up & running: Shipping reliable containers in production. O'Reilly Media, Inc., Newton, Massachusetts, USA.

Orzechowski M, Balis B, Pawlik K, Pawlik M, and Malawski M (2018). Transparent deployment of scientific workflows across clouds-Kubernetes approach. In the IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), IEEE, Zurich, Switzerland: 9-10. https://doi.org/10.1109/UCC-Companion.2018.00020

Ren J, Yu G, He Y, and Li GY (2019). Collaborative cloud and edge computing for latency minimization. IEEE Transactions on Vehicular Technology, 68(5): 5031-5044.
https://doi.org/10.1109/TVT.2019.2904244

Santikarama I and Arman AA (2016). Designing enterprise architecture framework for non-cloud to cloud migration using TOGAF, CCRM, and CRMM. In the International Conference on ICT for Smart Society, IEEE, Surabaya, Indonesia: 32-37.
https://doi.org/10.1109/ICTSS.2016.7792855

Seol J, Jin S, Lee D, Huh J, and Maeng S (2015). A trusted IaaS environment with hardware security module. IEEE Transactions on Services Computing, 9(3): 343-356.
https://doi.org/10.1109/TSC.2015.2392099

Tihfon GM, Park S, Kim J, and Kim YM (2016). An efficient multi-task PaaS cloud infrastructure based on Docker and AWS ECS for application deployment. Cluster Computing, 19(3): 1585-1597. https://doi.org/10.1007/s10586-016-0599-0

Yu L, Shen H, Sapra K, Ye L, and Cai Z (2016). CoRE: Cooperative end-to-end traffic redundancy elimination for reducing cloud bandwidth cost. IEEE Transactions on Parallel and Distributed Systems, 28(2): 446-461.
https://doi.org/10.1109/TPDS.2016.2578928

Zhao N, Tarasov V, Albahar H, Anwar A, Rupprecht L, Skourtis D, Warke AS, Mohamed M, and Butt AR (2019). Large-scale analysis of the Docker hub dataset. In the International Conference on Cluster Computing (CLUSTER), IEEE, Albuquerque, USA: 1-10.
https://doi.org/10.1109/CLUSTER.2019.8891000