DOCKERIZING VIRTUAL WIRELESS SENSOR NETWORK(VWSN):ISSUES AND SOLUTIONS

DOCKERIZING VIRTUAL WIRELESS SENSOR NETWORK(VWSN):ISSUES AND SOLUTIONS

VOLUME 7, ISSUE 1, 2021 (HTTPS://WWW.GYANVIHAR.ORG/JOURNALS/INDEX.PHP/CATEGORY/INTERNATIONAL-JOURNAL-OF-CONVERGING-TECHNOLOGIES-MANAGEMENT/VOLUME-7-ISSUE-1-2021-INTERNATIONAL-JOURNAL-OF-CONVERGING-TECHNOLOGIES-MANAGEMENT/)

Mohammad Equebal Hussain

[1]Research Scholar

Department of Computer Science and Engineering

Suresh Gyan Vihar University Jaipur, India

mdequebal.60508@mygyanvihar.com (mailto:mdequebal.60508@mygyanvihar.com)

Rashid Hussain[2]

Professor & Head of Department

Suresh Gyan Vihar UniversityJaipur,India

rashid.hussain@mygyanvihar.com (mailto:rashid.hussain@mygyanvihar.com)

***Abstract*— Wireless sensor network (WSN) is a group of distributed and dedicated sensors node connected with wireless communication device which is mostly used for monitoring and recording physical conditions[1] of environment, weather,temperature,sound,pollutions,insects monitoring, health monitoring etc. and organizing the collected data to a central location. Design of WSN depends on application requirements. WSN is a physical device.it can be implemented in virtual machine by separating data plane and control plane using abstraction from the hardware on which it runs. It heavily depends on virtualization to enable design usingsoftware.In this manuscript, we are focusing on the security challenges involved in adoption of container technology to implement WSN using docker as well as virtual machine.**

Keywords– ***virtual wireless sensor network; hypervisor; Docker container,virtualization.***

1. INTRODUCTION

The journey of computation has gone through lot of change from in premise data center to client-server architecture, distributed system to cloud computing. The purpose of all these transformations are to make better return on investment (ROI) as well as to scale up and scale down based on requirement in order to achieve high efficiency and improve business process delivery. Virtual wireless sensor network devices are not an exception. Many companies such as VMware, Amazon and Microsoft provide cloud solutions with lower cost and complexity, high elasticity and resource sharing.

Cloud computing are of four types. Public cloud (third party, low cost, less secure), Private cloud (No sharing, more secure), Hybrid (semi private) and Community cloud (Shared between organizations having common goal) [2]. Based on business need,onecandecidethesuitablemodelforitself.

Cloud services are mainly grouped into three categories[3]i.e.

IaaS (Infrastructure as a service) – Servers and storage on rent

PaaS (Platform as a service)–for developing, managing, testing and delivering software without worrying about internal infrastructure like server,networking, storage,database.

SaaS(Software as a service)–On demand software application managed by cloud service provider.

Cloud users can process and store data on the web using internet connection. Security is a concern in cloud computing platform. Based on some facts it is assumed that cloud platform is less secure than in house data center.

The proposed design of virtual wireless sensor network(vWSN) is based onconceptofvirtualmachine(VM)which is a software computer, runs an operating system and one or more application. (Fig-1) _ Interconnectivity among vWSN is a major challenge in the design.(Fig-2)

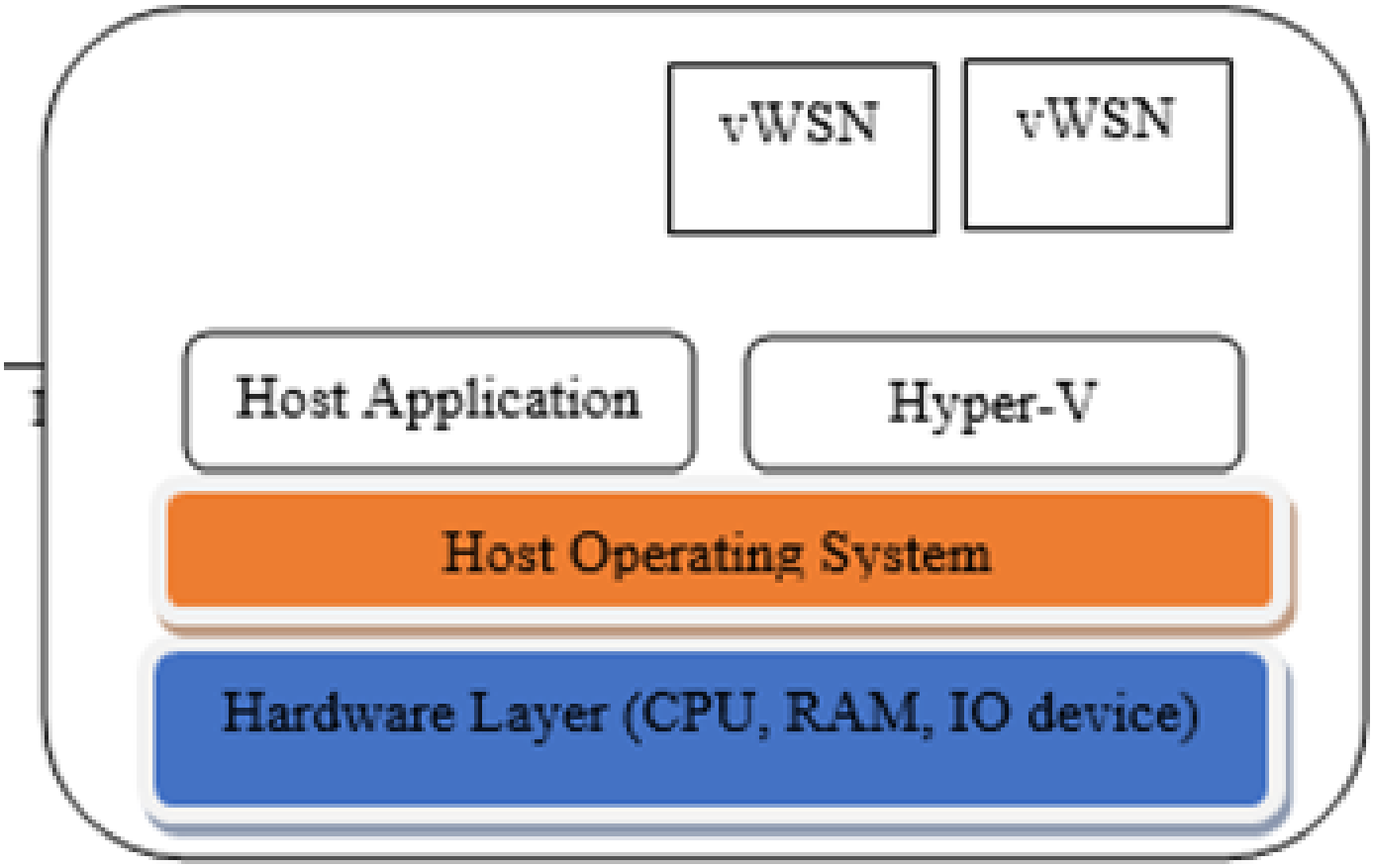


Figure-1

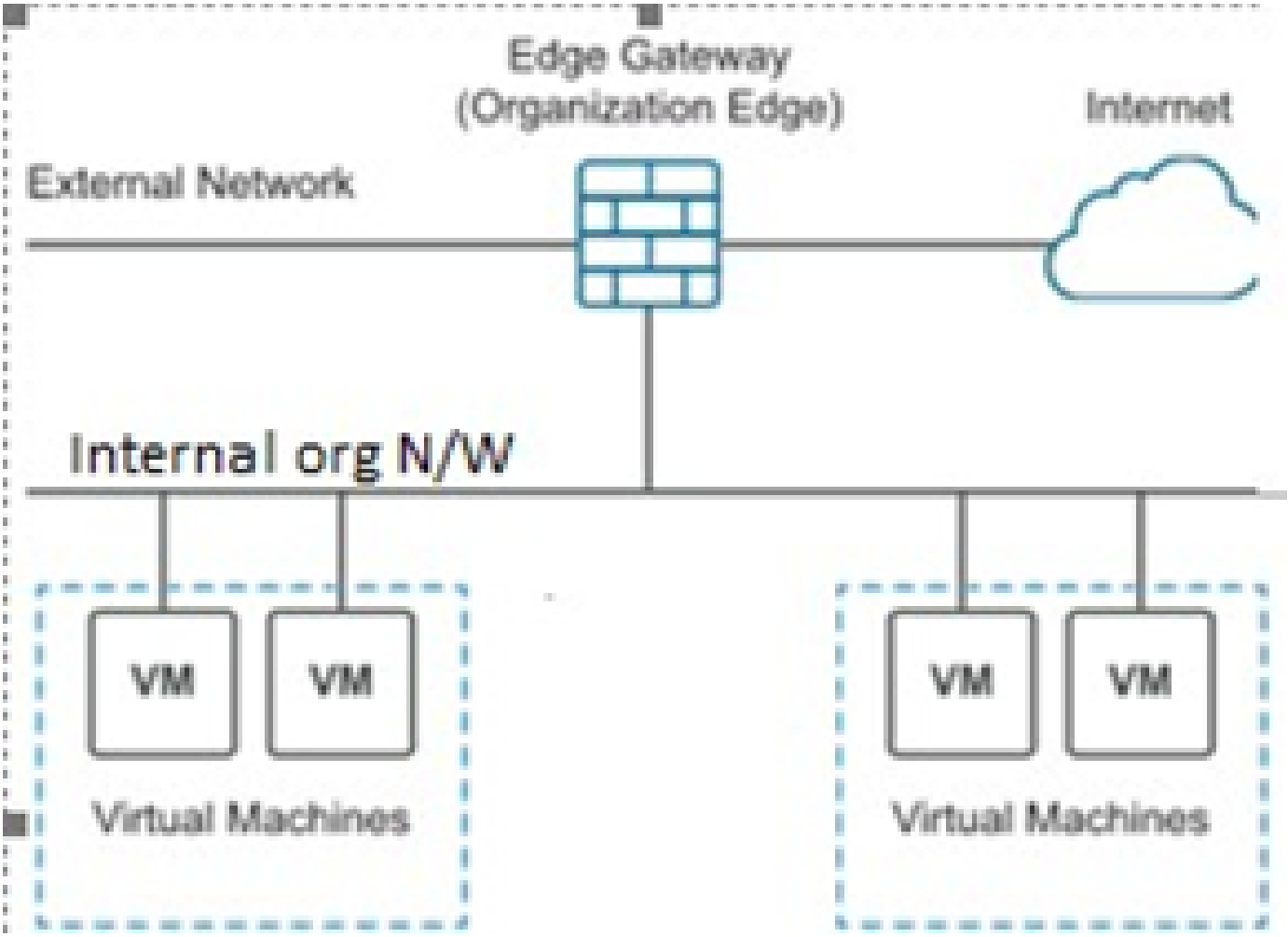


Figure-2

1. NETWORKSECURITYINVIRTUALWSN

2. *Securityofvirtualmachine*

By design virtual machines are isolated from each othertherefore multiple VMs can run securely while sharing thesamehardware[4].GuestOSinoneVMcandetectonlythosedevices which are made available to it. On the same host, oneVM failure is independent of other VM. Virtual machinesshare physical resources like memory, CPU, IO devices of thehost machine using VMKernel hence VM can't avoid thisisolation level. This is where possible security breach can't bedenied.

1. *VirtualNetwork*

Independent logical network between shared physical network is created using virtual network method. This is applicable across all hypervisor.

Isolation in virtualization is one of the key issues which plays crucial role in VMs to guarantee that one virtual machine(vWSN)cannot affect other vWSNrunning within the same host. Xen hypervisor which is an open source standard for virtualization is secure and widely used across multiple guest OS. Domain 0 is the first domain which is created when system boots. It has special privilege.

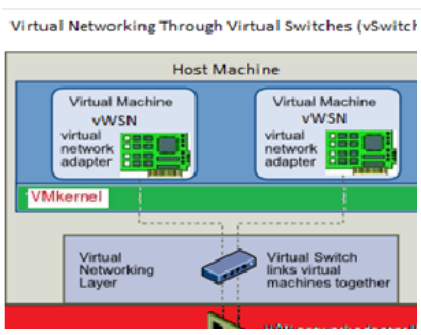


Figure-3

1. *Dockercontainer:*

Docker is a container-based solution to provide lightweight virtualization [5]. It helps to develop and scale the application fast and easy.

1. *virtualmachine.*

Docker avoids overhead of hypervisor layer therefore provides benefits of virtualization as well as improved performance. Dockercontainer contains everything required for running an application i.e.code, libraries, system tools, runtimeenvironments.However,securityissuesstillexistinadoptingdockerintheproductionenvironment. In this manuscript we will study possible securities flaw in dockercontainer and provides solution to avoid it. Below diagram explains the difference in architecture of virtual machine and dockercontainer.

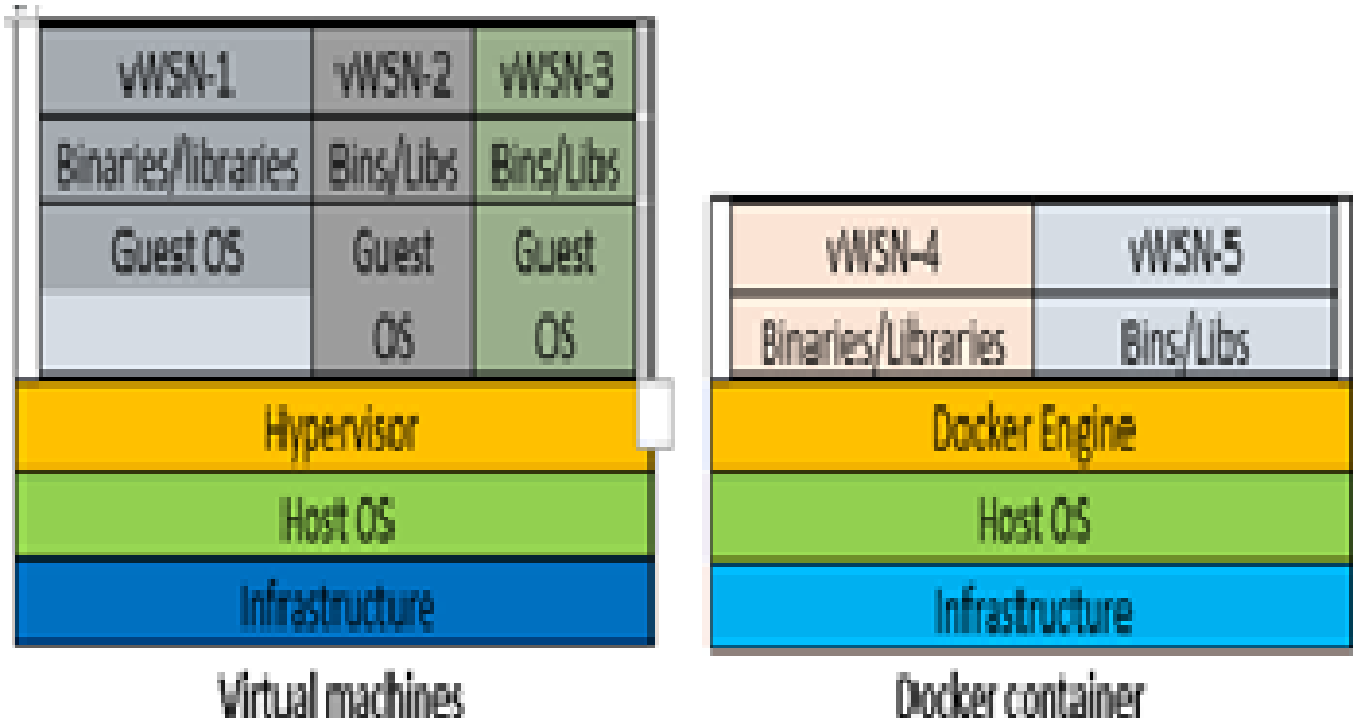


Figure-4

1. *VirtualNetworkVulnerabilitiesinvWSN*

Network virtualization is a technique to share physical network resource among different virtual networks. VMs interconnectivity is one of the biggest security challenges in design using virtual network which significantly affects security [6]. In order to isolate each VM, dedicated physical channel is the more secure way. Bridge and route are used to link VMs in virtual network. Therefore, chances are that isolation can be easily broken.

Following are the possible vulnerabilities which exists in thecurrentvirtualnetwork:

- Packet capture using sniffing virtual network:Various sniffer tools are available to sniff packet like wireshark because VMs share the virtual hub to communicate in bridge mode.
- Spoofing virtual network: Dedicated virtual interface (vif0) is used to connect each VM. Hence using Address Resolution Protocol (ARP) method it is possible to sniff packets betweenVMs.

ARP: $f(IP)=MAC$

Below figure illustrates how does spoofing works in virtualization environment. Using ARP, convert an IP address into a matching physical address. When virtual routes start, routing table is initialized due to sending ARP command to each VM during boot time.

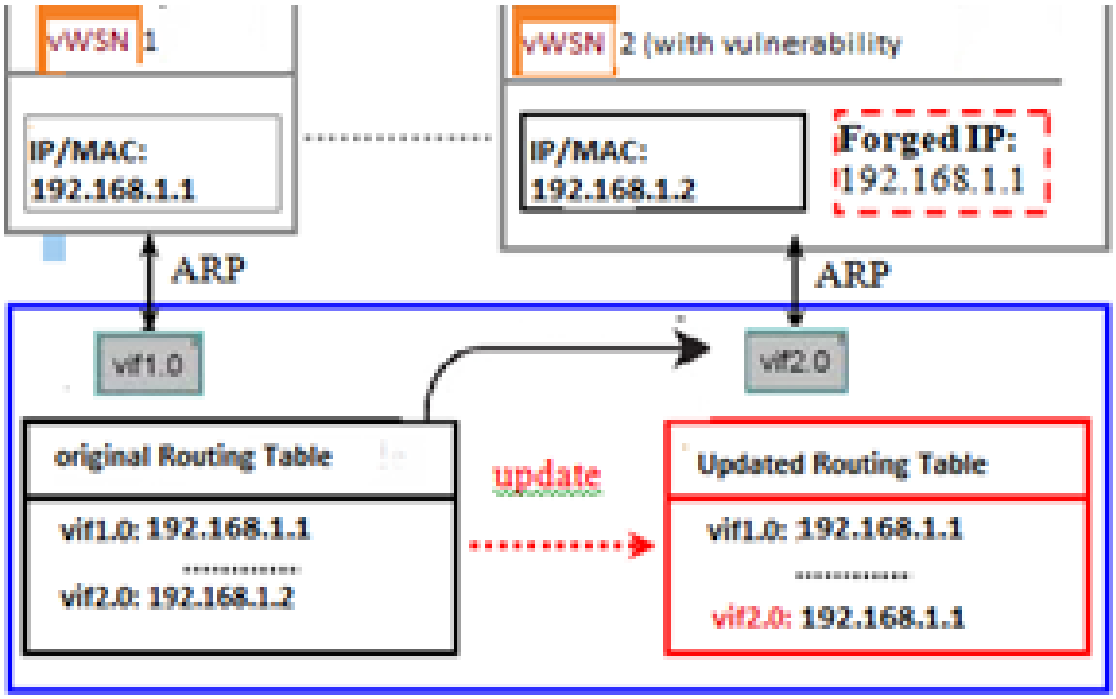


Fig. Spoofing in virtual sensor network

Figure-5

In above example,it can be observed that how ARP spoofing attack is launched by vWSN2 by forging same IP address with another VM, vWSN1 that sent an ARP to virtual route [7]. As a result, the virtual route gets updated by latest information received from vWSN2. Because of this, traffic which is destined vWSN1 will now be sent to vWSN2.Which is a possible security breach.

- PROPOSED VIRTUAL NETWORK MODEL FOR VWSN

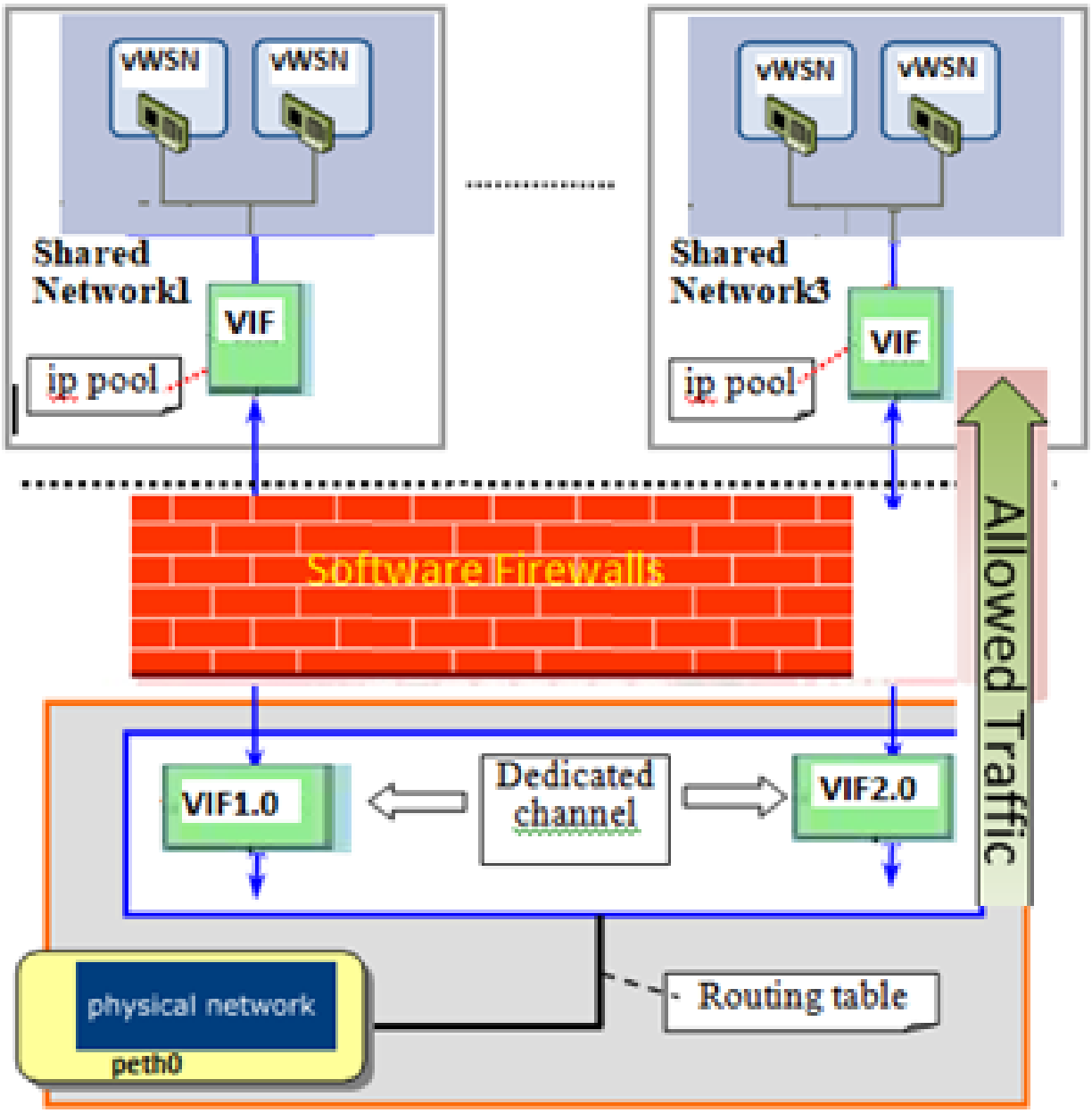


Figure-6

1. DOCKERIZINGWSN

Keeping in mind the various vulnerabilities that could exists in virtual network, we are proposing below model to make communications among VMs more secure. This modelconsists3-layerarchitecture.

- Bottom Layer (Routing) – connects between virtual network and physical network using dedicated logical channel. Assign unique id to each vWSN which can best or ed in a configuration file and used during communication.

exportUNIQUE_ROUTING_ID=1

- Middle Layer (Firewall) – It prevents unauthorized access to private network.This is achieved using access control list(ACLrules)which allows to inspect each inbound and outbound packet once arrives at virtual interface (vif) whether to allow, monitor or block the packets. ACL rules and policies are definedat firewall layer which assures secure communication between virtual interface and virtual shared network.
- Top Layer (Shared Network) – This allows to block the communication among vWSN within the same virtual shared network.This can be achieved by putting each virtual shared network in auniquesubnet. Whenever there is a communication required betweenVMs,the normal rules apply.

Below diagram illustrates the concept mentioned above.

Docker is introduced in 2012,but docker container has gained momentum recently in the industries.Dockercontainer provides an alternate way of virtualization which islittle different than hypervisor based virtual machine. It is light weight process that are isolated from other running application process. Docker is developed on the concept of namespace [8]. Resources are visible only to those processeswhich run on the same namespace. Process running in onenamespacesay‘X’can’t see process

running on an other namespace 'Y'. This provides a kind of virtualization and isolation of resource.Each container runs in its own namespace.This support is provided by the kernel which know sabout the namespace and duringAPIcall,kernel makes sure that process can only access resource of its own namespace.Containers are Flexible(can contain complex application), Lightweight (Due to sharing of host kernel),Portable (cloud deployable), Efficient, Loosely coupled (can be replaced easily without disrupting other containers),Upgradable (each container can be upgraded independent ofothercontainer),Scalable(elasticnature)andSecure.

Docker shares host kernel therefore the size is much lower compared to hypervisor based virtual machine. It is extremely fast and superior in distribution of application. Sharing ofkernel is the single point of failure. Hence the security breach inside a container can compromise the security of host kernel.Breakdown of one container can affect the other container running in the same system.

Securities issue in containers are the biggest concern for enterprise.

1.

	Dockercontainer	**Virtualmachine**
Isolation	OSlevel	Hardwarelevel
Sharing	ShareOS	SeparateOS
Performance	Light weight(MB), quickbootup	Heavy weight(GB),moretimetobootup.
Availability	Pre-builtcontainersare available	NoreadyVM
Createtime	Less	More
Resourcerequirement	Less	More
Runtime	Dockercanrun withinaVM	n

- DOCKERCONTAINER VS.VIRTUALMACHINE

1. ANALYSISOFDOCKERSECURITY

As far as security is concerned, each VM has its own operating system. There is strong isolation in the host kernel therefore VM are more secure than containers. Container has lot of security risk because of shared host kernel [9][10].

Attackers can exploit all containers in a cluster if get access to one container. However,inVM,hypervisor layer restricts there source usage.

- DOCKERSECURITIESISSUESANDSOLUTIONS
    - **Docker + virtual machine combination**: Process running in VM is more secure than process running in a docker container because VM is 2 layer up i.e. vmkernel and hypervisor layer to reach host kernel. Whereas docker container is just one layer upon host kernel. Hence a small vulnerability in application running on docker container can bring down the host kernel. Hence solution to this problem is to deploy container inside aVM as shown below.
- **Allowing limited privilege to running container**. Avoid–privileged flag which gives all capabilities to the container.Also lifts all limitations enforced by device group. give specific capabilities using –cap-addflag. dockerrun–privileged-t-i–rmubuntu:latestbashroot@50e7aeb:/#cat/proc/sys/vm/swappiness60

root@50e7aeb:/# echo "61" > /proc/sys/vm/swappinessroot@50e7aeb:/#cat/proc/sys/vm/swappiness

61<<<<<change the hosts kernel parameters

- **Limiting the number of vCPU**– By default all containers get equal number of vCPU [11]. This proportion can be adjusted by making change in configuration file.
- **Read only setting to file system wherever possible**.Keeping file permission as Read only

(4)for all those files which doesn't need modification.

- **Turn off intercontainer communication wherever possible**.This could be achieved by setting the flag"–icc=false".By default, network traffic between containers in the same host is not restricted[12].That could create a security issue.Defining new flag or using the existing flag could possibly solve this problem.
- **Memory limitation of a container**: Limiting the total amount of memory container can use is very much required to prevent other container running out of resource. There exists an attribute or flag to achieve that goal.

Resources:

memory:"300M"cpu:"100m"

- **Trusted image**: The official registry for dockercontainers has many images to download whichmay be from untrusted source [13]. The available images could contain malicious code which attacker can use to gain access to the system and data.
- **Managing Secrets:** containers are created for application which may need access to database and other important services available on the host.Most of the services need credentials. If an attacker gain access to these secrets, then securitywill get compromised [14]. To keep passwordsecure, following preventive measures arerequired.
  - No environment variables to store secrets
  - Keep secrets files inside k8s/directory.
- CONCLUSION

Docker containers are assumed to be less secure than VM, hence adopting this in production is prevented. Major security issues are the malicious images in docker registry hub, denial of service attacks. Most of the securities issues can be prevented by using precautions discussed above. Going forward these issues will be addressed and resolved.

1. ACKNOWLEDGEMENT

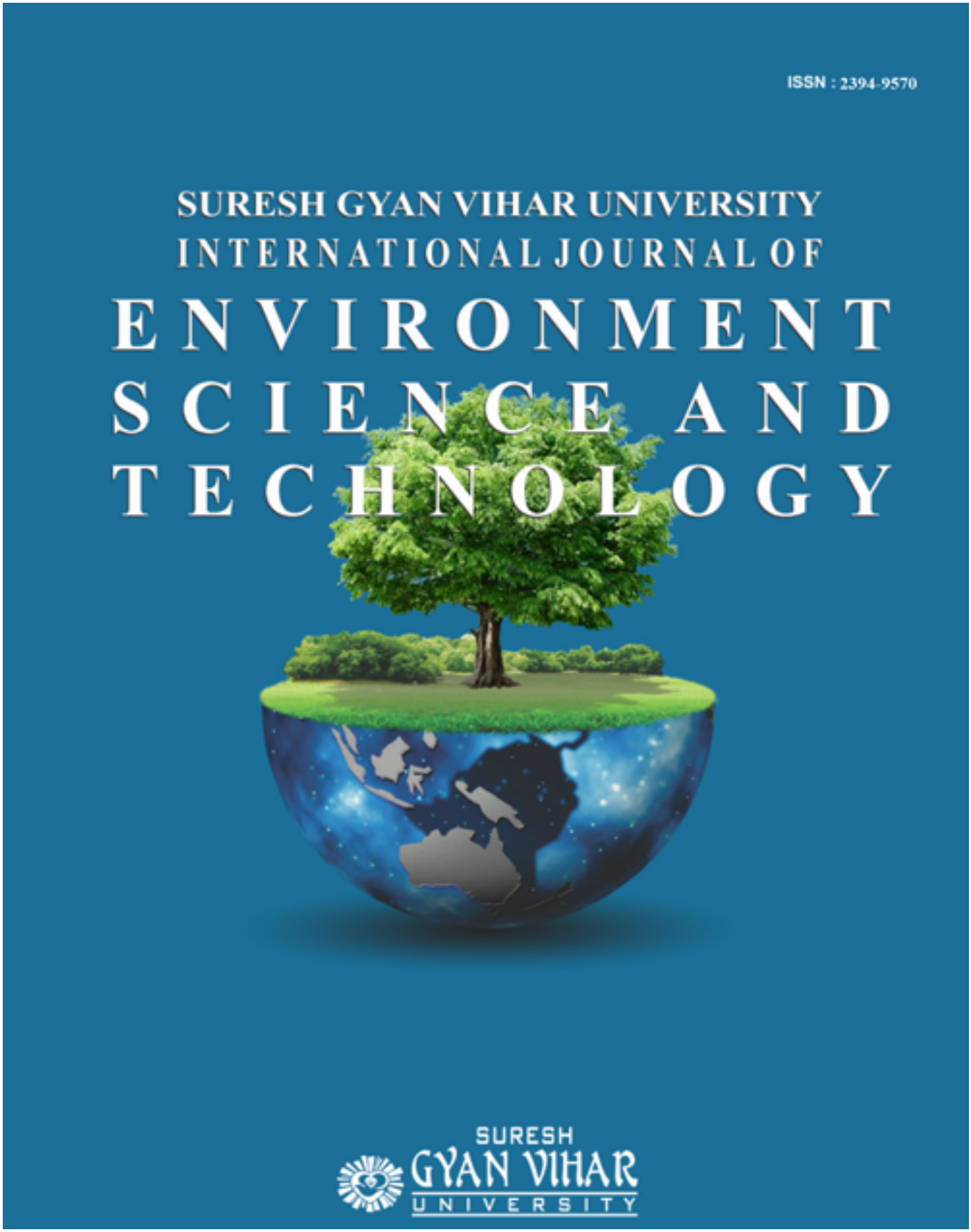
We thank Professor Dr. Rashid Hussain (Suresh GyanViharUniversity, Jaipur Rajasthan India) for their valuable suggestion and constructive comments that helped substantially improving the paper.

1. REFERENCES

- Binh,H.T.T.,&Dey,N.(2018). Softcomputinginwirelesssensornetworks.CRCPress.GoogleScholar (https://scholar.google.com/scholar?q=Binh%2C%20H.%20T.%20T.%2C%20%26%20Dey%2C%20N.%20%282018%29.%20Soft%20computing%20in%20wireless%20sensor%20networks.%20CRC%2
- J.R,Dr.S.Vijayalakshmi"AStudyonCloud Computing and Hybrid Cloud" Vol. 68 No. 19 (2020):NationalConferenceOnMulti-DisciplinaryApplicationPerspectiveinIoT
- Qian, Z. Luo, Y. Du, L. GuoCloud computing: anoverviewSpringer (2009),pp.626-631
- V. Radhika,Krushna Chandra GoudaS. SathishKumar (2019). "Priority Based Virtual Machine Allocationand Scheduling for Security in Cloud Computing"https://link.springer.com/book/10.1007/978-981-32-9690-9 (https://link.springer.com/book/10.1007/978-981-32-9690-9)pp617-625
- Ruchika,V.:EvaluationofDockerforIoTapplication.Int.J.RecentInnovat.TrendsComput.Commun.**4**(6)(2016)
- VaishaliSingh,S.K.Pandey(2019)"CloudComputing:Vulnerability and Threat Indications"https://link.springer.com/book/10.1007/978-981-13-8253-6 (https://link.springer.com/book/10.1007/978-981-13-8253-6%20pp%2011-20)pp11-20 (https://link.springer.com/book/10.1007/978-981-13-8253-6%20pp%2011-20)
- TanmoyMukherjee,SudiptaSahana,DebabrataSarddar(2019)"ANobleApproachTowardSecurityImplementationin Cloud Virtualization Framework"https://link.springer.com/book/10.1007/978-981-15-0829-5 (https://link.springer.com/book/10.1007/978-981-15-0829-5)pp541-552
- https://docs.docker.com/engine/docker-overview/ (https://docs.docker.com/engine/docker-overview/)
- https://www.stackrox.com/post/2019/09/docker-security- (https://www.stackrox.com/post/2019/09/docker-security-101/)101/ (https://www.stackrox.com/post/2019/09/docker-security-101/)
- AdrianMouat,"DockerSecurity-UsingDockercontainerssafely",O'ReillyMedia,August2015

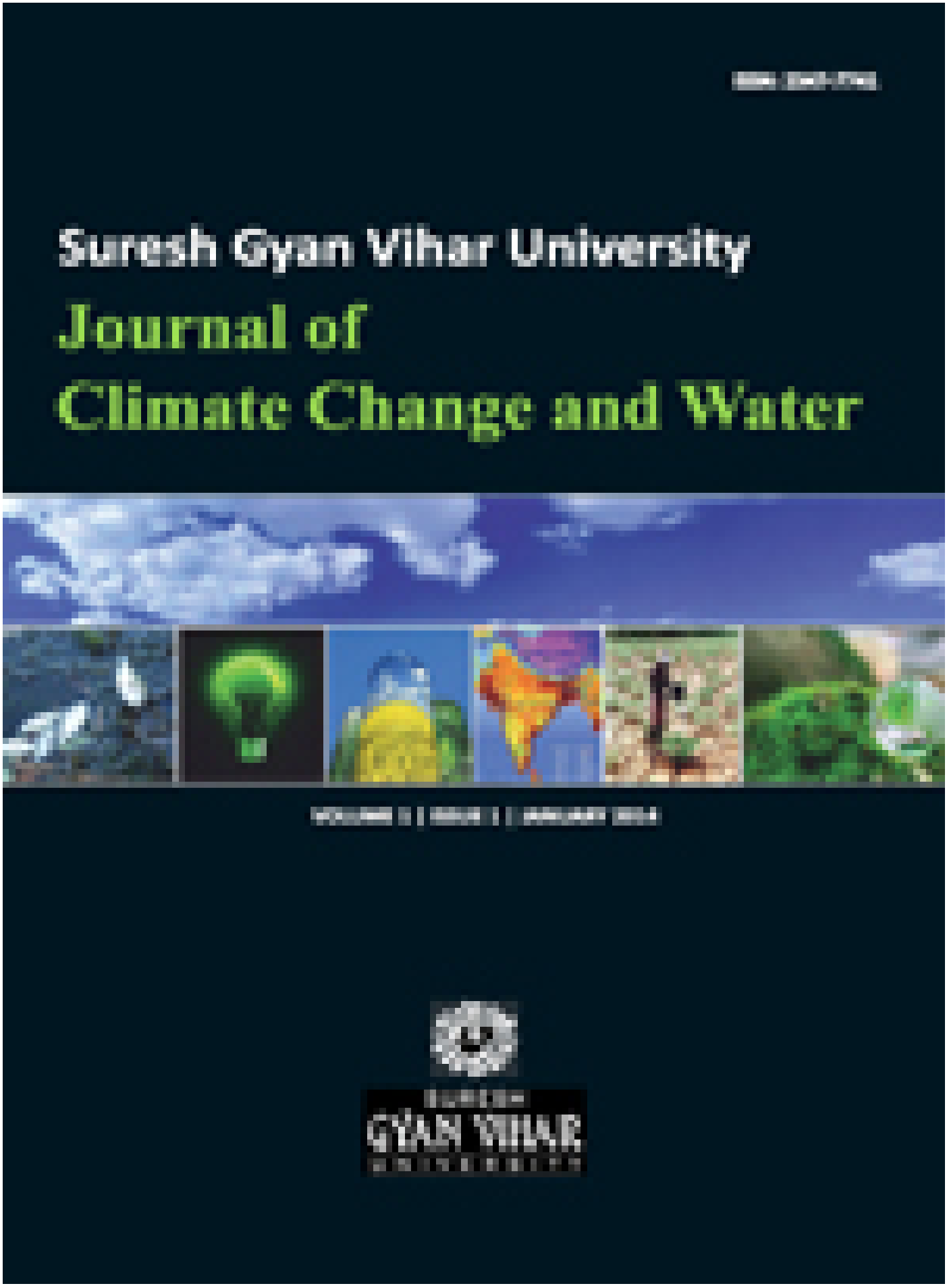
- Jessie Frazelle, Docker Engine 10 SecurityImprovements, February 2016,https://blog.docker.com/2016/02/docker-engine-1-10- (https://blog.docker.com/2016/02/docker-engine-1-10-security/)security/ (https://blog.docker.com/2016/02/docker-engine-1-10-security/)
- Marek Goldmann, Resource management inDocker, https://goldmann.pl/blog/2014/09/11/resource-(https://goldmann.pl/blog/2014/09/11/resource-management-in-docker/#_example_managing_the_cpu_shares_of_a_containe)management-in-(https://goldmann.pl/blog/2014/09/11/resource-management-in-docker/#_example_managing_the_cpu_shares_of_a_containe)docker/#_example_managing_the_cpu_shares_of_a_containe (https://goldmann.pl/blog/2014/09/11/resource-management-in-docker/#_example_managing_the_cpu_shares_of_a_containe)
- SusanHall,"DockerContainerSecurity:Signed,SealedandDeliveredfromVulnerabilities",November2015,https://thenewstack.io/3-new-security-features-docker/ (https://thenewstack.io/3-new-security-features-docker/)
- Jinjian Yu, ChuanJia, Dong Pu"A Review of DockerSecurityResearch"https://doi.org/10.12677/csa.2019.95105 (https://doi.org/10.12677/csa.2019.95105)

(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/ENGG.PHP)



(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/ENVIRMENTAL_SCIENCE.PHP)

(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/CTM_JOURNALS.PHP)



(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/INT_JOU_CLIMATE_CHANGE_WATER.PHP)

(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/ECO_MANG_JOUR.PHP)

(HTTP://WWW.GYANVIHAR.ORG/RESEARCHJOURNALS/PHARMACY.PHP)