Journal of Theoretical and Applied Information Technology
31st May 2019. Vol.97. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPREHENSIVE ARCHITECTURE FOR SECURING VIRTUALIZATION ENVIRONMENT IN AN HYPER CONVERGED SYSTEMS

[1]DR. AHMAD RAZA KHAN

[1]Assistant Professor, Majmaah University, College of Computer and Information Sciences,

Department of Information Technology, Al Majmaah

Kingdom of Saudi Arabia

E-mail: [1]ar.khan@mu.edu.sa

ABSTRACT

As virtualization enhances the use of computing and scalability of computing resources it's important to secure these resources and the applications which are running on the virtualization environment. Most of the small and medium scale businesses are switching over to virtualization environment so that the capital expenditure CapEx can be reduced and the operational expenditure Opex can be increased this can be achieved only by switching to the virtualization environments running multiple machines on highperformance services or hyper-converged environments. As a huge number of virtual machines are running on the virtualization environment it becomes critically important to protect each virtual machine from getting attacked by various intruders such as attackers, viruses, and malware. In this research we are proposing a comprehensive architecture and deployment method for virtual machines on the hyperconverged environments so that data and applications running on the environment will be protected from the attacks that are taking place and also thin provisioning of the virtual machines so that exact capacity of the disk storage is available to the virtual machine to compress its data on the virtual image or the .vmdk, .nvram and .vmem files which are stored on the hyper-converged environments

Keywords: *Virtualization, security, virtual machines, hyper converged, cloud computing*

1. INTRODUCTION

Most of the companies are investing a lot of money in providing adequate computing resources to the employees who are working on the project which are running in the company many companies invest hugely in IT infrastructure so that the employees can be more productive and can use the latest technology for completing the ongoing project in the companies. But as the technology advances companies need to buy new IT infrastructure for supporting the new technology to execute their projects. This is creating a lot of capital expenditure on the small and medium scale business to procure new IT resources every time to run the projects. Also, the employees demand from the IT to give them high resources and good infrastructure to work so that the computer systems do not lag in completing their work in time also the machines should be scalable to suit the project requirements. Thus, it's important that companies should switch over to the Virtualization and cloud computing environments that best suits for business process implementation. Visualization of infrastructure is Becoming more popular in Business to Business Integration and also Business to Process Integration it's important for the developers to protect the mission-critical applications which are running on the virtual machines that are deployed on the hyper-converged platforms such as VMWare solutions for virtualization. One of the most important factors influencing the use of virtualization is scalability of the infrastructure on the fly if the end users and developers of an organization are using virtual machines to complete some project work they may require to scale their virtual machines configuration so that there is no latency in running the workload.

Virtualization technologies provide huge resource warehousing where they maintain three different types of resources which can evolve over time and with the budget to grow these resources. Following are resources which are pooled together by the virtualization systems include:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Compute Resources Pooling
- Storage Pooling
- Platform Pooling

These resources are mainly required by the software development team and other stakeholders who are involved in the project execution and project management activities. It's important to secure these resources so that attackers and malicious software do not attack the system and information are leaked out from the system to the outside world. Information flow between the virtual machines need to be a source and also need some encryption algorithms to be implemented so that information that resides in the virtual machines are not easily understood by the attackers. A hyperconverged platform from various virtualization providers are now more compact and provide interoperability with different services which exist in the virtualization box that is built to cater requirements or huge companies and their evergrowing needs for IT resources.

2. HYPER CONVERGED SYSTEM DESIGN IMPLEMENTATION AND SPECIFICATIONS

Hyper-Converged Systems are being deployed in large and small organizations today to speed up development and deployment infrastructures and to provide adequate resources to the IT professionals who are working on the client's project so that they do not find any latency in completing the working using the IT resources which are provided by the organization. Businesses are investing huge amount of money in pooling resources which can help developers to complete their work on time and within budget.

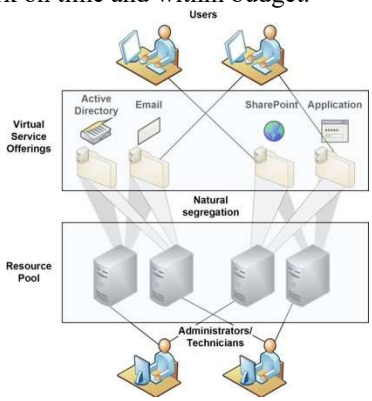

Figure 1: Resources Pooling by different applications in Business Process Integration Model

The confluence of best in business technologies such as compute storage and networking working together to solve the problem of resource management and resources pooling can be overcome using the hyper-converged technologies also the IT engineers get an ability to manage their workloads across different virtualization and cloud computing environments. Servers being an important factor for building the IT infrastructure it's important that IT engineers should focus on how the servers interact and exchange information so that the information packets losses are avoided and the system is more stable and does not have any downtime. In a hyper Converged environment, there are large building blocks which work together such that the IT engineers find no downtime in the system. The hyper-converged racks which are also called blocks can be integrated to multiple tacks which provide backup and fault tolerance capabilities so that the IT infrastructure is up and running 24x7 without any downtime.

Figure 2: A hyper converged Infrastructure with CI Building Blocks

The figure 2 above shows how the IC Block uses different resource pooling capabilities such as storage which is VSAN in the above case and compute capabilities which is implemented with the help of hypervisors on top of the physical pool of computing resources and the network pooling with is accomplished with the help of NSX and configuration environments all these resources will collaborate with each other to provide highly efficient and scalable infrastructure for the IT project managers.

As hyperconverged systems are collocating information from different resources which are located geographically apart from each other and require to share resources which can be shared between different projects in the same organizations or can be between different organization can be done using the secure transport protocols and information can move from one virtual machine to the other virtual machine without any security related issues as the as the virtual machines are in the compressed states which can only be accessed by legitimate user who is having the credentials for accessing different resources in the organization. As huge data resides

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in the data centers today its important to manage resources and at the same time allow data to blow between various virtualization environments its important factor affecting the industry today. Resources and the data should be pooled from different sources which can later be accessed by the required resource person in the company.

Hyper converged systems offer lots of services which can be accessed by different pool of users who have access to the data residing on the virtual machines which have been deployed in the virtualization infrastructures hyperconverged system allow system administrators to combine and manage different resources under a single platform which in turn results in easy configuration of resources and easily accessing different sources of data from the virtualization machines. As the companies are more focused on the operational expenditure which will yield to high productivity and will increase the performance of the productivity for the company at large. Large amount of computing resources are available in the company but the issues is that it's difficult to keep track of all the resources an provide a statistical report of which resources are consuming which other resource and at what time thus the administrators need to maintain a history of all the resources which are available in the company and when they should be available so that the uptime of the resource can be made available to the requesting resource. With the help of hyper converged systems now it's easy manage all computing resource under a single shelf which is the datacenter which contains different VxRail machines that are deployed and can be customized based on the client requirement so that the end user will have privilege of using different machines and managing them using a central graphical user interface system so that it's easy to keep track of the machines running on the hyperconverged infrastructure and the systems can be allocated and deallocated resources based on the clients requirements.

On the other side, it's important for a large business to pool similar resources such as storage, computing and networking into big racks which can be easily manageable and deployable this can be achieved using the HCI (Hyper-Converged Infrastructure) Racks which provide the confluence of multiple resources in the same rack space. The HCI appliances which are the pooling resources need to work in coordination with each other so that optimum performance can be achieved these racks provide interconnections between different resources which are available in the organization. Each system which is deployed in the HCI has a system boundary each of the HCI appliances can be scaled and grownup to meet the requirement of the client.

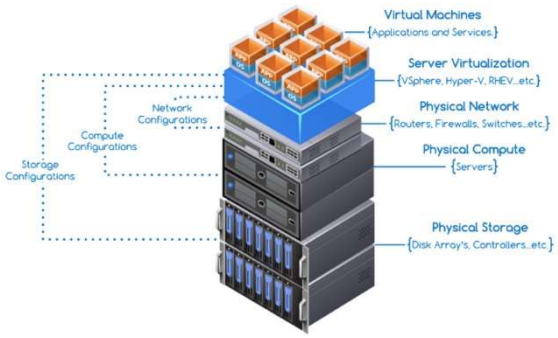

Figure 3: A hyper converged Infrastructure redundant SAN's and redundant virtualization servers

In the figure above, we can see how the physical storage devices are connected to the redundant disk array containers. These storages are configured in the server virtualization environment and the hypervisor will allocate the disk of arrays and will provide storage resources to the virtual machines which are running or while designing the virtual machines online. This array of disk will be helpful in allocating resources to the virtual machines which are running out of disk this can be achieved dynamically. The compute which resides above the storage of the virtualization environment will provide computing resources to the virtual machines these computing resources will be merged using the vSphere hyper-converged environment and the set will be configured to use comprehensive computing power for all computing boxes will be used for creating the virtual machines which are requested by the developer and the other stakeholders working in the company.

Storage being one of the most important concerns in the hyper converged environment data residing in the SAN's should be available to the end user frequently of based on the request of the client and the machine which is requesting the storage to be accessed over due course of time it's very important that the system should be available and running 24x7 without any downtime which may cause loss of data which is being accessed by the virtual machine clients thus keeping data up to date and close to the physical servers so that the hops to access the data using the network is reduced. The hyperconverged infrastructure provides the organization with centralized infrastructure management and deployment mechanism this will enhance the performance of the IT infrastructure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which can be assessed by the organization's IT administrator easily. As most of the configurations which include storage, network and compute are all available under the same server rack which creates a easy to configure and easy to manage system for the administrators of the company also its easy to keep track of resource which are being consumed by the users within the organization and also outside the organization. Configuration of these resources is done using the single graphical user interface which allows the administrators to deploy resources in the hyperconverged infrastructure easily and also to allocate and deallocate resources form the users requesting for the resources easily this will improve the efficiency of using the resource as an when required by the system engineers working the company.

The servers which are running the hyperconverged infrastructure have huge processing capacity around 96 cores can be deployed on a single rack server which can run different applications and the performance can be increased in the hyperconverged environment by adding more CPU's and the Memory which will enhance the usage of the system and will increase the performance of the virtual machines which are running different applications on the core side also during the peak performance time the capacity of the resources can be increased and the processors can be configured to run at maximum flipflops which when the enhance the performance of the application which is running in this environment. Dynamically allocating and deallocating or resources can be done and the users can be given privileges to access the resources on the virtual machines as an when the request for the resource is increased information regarding the resource utilization and the virtual machines running in this infrastructure can be monitored and efficiency of the hyperconverged environment can be measures if there is a need to increase the resources to improve the performance of the hyperconverged system then the administrators can request for increasing the CPU, RAM or the disks so that the performance which is required by the machines can be fulfilled.

Migrating data and the virtual machines can be achieved using the vcenter product provided by the vmware company this is help migrating data securely in a live environment and without any downtime to the system. If the clients are running virtual machines are required to be moved from one data center to the other this is easily possible using the virtualization environment which is created on the hyperconverged infrastructure data redundancy and data duplication this will save a lot of time for the administrators and the clients running the applications on the hyperconverged environments collecting information regarding the data and the vm's running on the system can be done by the admins of the system and the admins can decide a time when the migration can take place so that incase if data is corrupted or lost can be backed up from the original servers.

Resource management and allocation has become easy with the help of hyper converged infrastructure as the number of virtual machine users are increasing and the huge demand for compute and storage is increasing from the developers who are working on different applications which are residing on the hyperconverged infrastructure of the company its important to keep track of all the resource which are being utilized and the resources which are not being utilized by the company at large so that the unallocated resources can be reutilized and the made available to the requesting vm's in the company as the organization grows large and the systems are increasing the information regarding the management of the resources is also increasing data needs to be kept in a secure environment where the legitimate users can only access the data the other users are not allowed to access any resources and the data without authenticating their identity to the system.

As all resources such as compute, storage and networking are virtualized in the hyperconverged environment its easy to manage and maintain the resources and also to keep track of all the resources from a central user interface which is provided by the hyperconverged companies. configuring the hyperconverged resources has also been made easy as the graphical user interface provides all information regarding configuration and deployment of resources when required by the infrastructure it's also easy to manage and maintain the resources in case any maintenance is required by the administrators of if the resource are falling short for the users of the vm's the system will generate alerts which can be then handled by the administrators and based on the request generated by the system more resources can be allocated to the system. Thus the clients running their applications on the virtual machines will never fall short of the resources which is computer, storage and networking.

Data management in this infrastructure is also a big challenge as all the resources are converged and the data resides in different applications and most of the applications are requesting for data from different sources its

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

important to manage and maintain all the resources such that if the data is required by one system which is running. Virtual machines can be accessed by the SAN's easily and no latency is incurred in the system for accessing the data and the information is easy to collect and collaborate with.

3. SECURING VIRTUALIZATION DESIGN INFRASTRUCTURE FOR RUNNING VIRTUAL MACHINES

As virtualization involves many components which are integrated to each other they are provided by different vendors it's important to secure each channel which could be a possible attack which can take place in the virtualization environments. Each vendor provides updates for the security of their products it's important to check for the security updates and the firmware updated for the devices which together build the virtualization infrastructure all patches from the vendors need to be checked and updated so that no flaw can enter the virtualization infrastructure and it would not be attacked by malicious software

In large organizations and businesses, multiple virtualization environments exist that hosts hundred and thousands of virtual machines these virtual machines need to be accessed remotely and the stakeholders connect to the virtual machines residing on the hyper-converged environment remotely. The bottleneck here is that the virtualization networks are likely to be attacked by the viruses and malware. So it's important to protect the network channel so that the stakeholders do not face any difficulty in accessing the virtual machines from remote locations of their offices.

As all resources are collaborating in the hyperconverged infrastructure it's important to keep track of all the processes which are requesting for the data and resources should be allocated on demand to the client all the resources should be monitored carefully so that the attacks on the systems can be reduced. As large businesses have huge applications and mission critical applications running on the hyperconverged systems it's important to keep track of each data point and each resource using the data point so that no bottle neck is possible for the attackers to attack the machine. Data being the CenterPoint for the mission critical applications should also be available to the applications when ever they need it with channels of transmission as the network is virtualized in the hyperconverged environment it becomes easy for the administrators using the tool for monitoring the virtual networks which have been created using the hyperconverged infrastructure the system utilizing the virtual network can also be monitored using the tools provided by the hyperconverged companies data flowing back and forward from the system needs to be tracked and the information needs to be handled carefully so that the possible attacks can be reduced in the hyperconverged environment.

As more and more companies have the office located across the globe it's important that the stakeholders get access to their virtual machines round the clock this will improve the productivity of the company and also the efficiency of the work will improve. the administrators are responsible for creation and allocation of resources for the virtual machines which are running online some time the administrators can not shut down the virtual machine to allocate resources to it at such time they have to allocate resources to the machines that are online and are being used by the stakeholders around the globe these mission-critical machines need resources in case they are running out of resources to complete their tasks on time without any delay for the further computation of data.

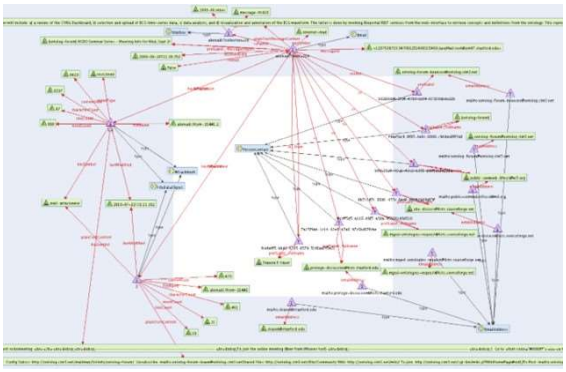

Figure 4: Analytical representation of multi-node hyper converged Infrastructure connected virtualization servers in business domain

The above figure shows who the virtualization systems are interconnected over large WAN network for businesses who have offices if different locations also the stakeholders would like to access their virtual machines from different networks residing on the client side. The network administrators need to provide secure access channels from where the virtual machines can be assessed from the stakeholder so that in case any virus or malware found on the clients machines cannot effect the other virtual machines running on the same platform most of the time the virtual machines which are running on the hyperconverged infrastructure are designed such that they are isolated from each other so that incase if one machines has been compromised by the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacker or any malicious software has attacked the virtual machine it will not affect other virtual machines running on the same virtualization systems. As the number of users are increasing in the business every day in and out its important to monitor each node in the network so that the security can be maintained its important to keep track of information movement between the nodes so that data can be kept secure.

As the companies are growing the demand for infrastructure is also growing and new application design and developments are more resource consuming so the developers and the product designers working of the company are demanding more infrastructure utilization and more resource allocations so that the applications run without any latency. Huge applications also demand for more network traffic so data dissemination so virtual networks are deployed on the hyperconverged infrastructure. Data collaboration between different teams in the organization also increases resource utilization and also there is a need to allocate more resources for running applications and other's too.

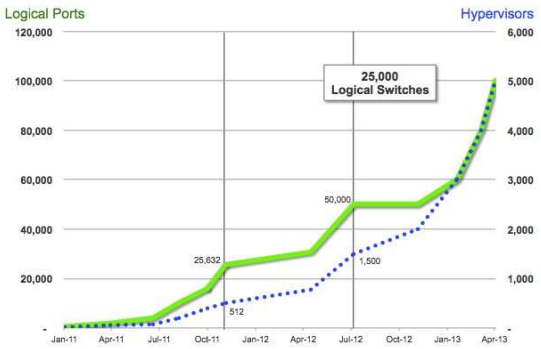

Figure 5: Graphical view of hypervisors and logical switches connected on the network and the logical ports open

The above graph shows how the hypervisors running on the virtualization environments and logical ports that are open for the VM's running on the local switches are increasing month by month this is important from security perspective as the number of notes connecting each month is increasing and the security risk to manage these resource allocations for the virtual machines is also increasing. It's important to keep pace with the ever-increasing demand of the stakeholder's performance requirements and the improving the efficiency of accessing the virtual machines over the network

Virtualization of resources which are connected to provide performance and enhance productivity in the organization need to be protected against attacks. As the number of virtual clients keep on increasing based on the requirement of the developer and other team members working in the company the administrator needs to server all these requests so that the project on which the company is working will receive all the resources necessary for executing the project on the client side. The resource utilization increases the demand of other shared resources such as the virtual network and virtualized CPU which will be catered to the client on demand. Securing this newly created infrastructure for any given project is an important task for the system administrator all resource such as compute, storage and network need to be secured from end to end so that the attackers do not find any means of attacking the system with unsecured infrastructure. Reliability is also a major concern in data sharing between different resource which are residing on the hyperconverged environment all the software's and the hardware's which are being shared as resources should be from legitimate and authentic sources so that they in themselves will not provide a bottleneck for the attackers to add malicious code in the resources which are being used by the company stakeholders. This level of security will involve all the vendors who have provided their infrastructure for designing the hyperconverged system and development can be then analyzed by the team of analyst who can confirm their integrity and security related issues. One of the most important reasons to build secure hyperconverged infrastructure is not only providing internal security from the company stand point instead all the infrastructure elements which together build the IT hyperconverged systems should also be secure so that the end points which are utilizing this hyper converged technology can also be secured and developers can work flawlessly without bothering about the infrastructure level security which is taken care by the system administrators at their end.

4. RESULTS AND DISCUSSIONS

As this research enhances security of hyper-converged systems by improving the architecture for resources allocation to the stakeholders who are working on client's projects and need good performance machines to run the workloads of the clients and to deliver the required output to the client without any latency in the work under process. This architectural design will improve security without compromising on the performance of the virtual machines which are running mission critical applications for the clients.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

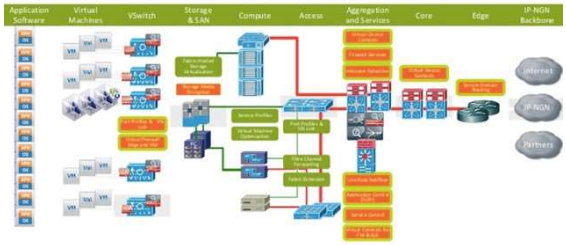

Figure 6: Secure architecture for hyper-converged environment

The figure 6 above show the architecture for protecting hyper-converged environment for getting attacked by malicious software's and intruders who can gain access to Virtual SAN and Virtual LAN which can now be protected as give in the figure 6 above. The resources can now be increased on the fly for the developers who are working on the virtualization machines and network administrators can protect the virtualization environment by adding a simple level of security to their systems this architecture improves security without compromising on the performance of utilizing the virtual machines on the hyper converged environment. This system also ensures that all the infrastructure related equipment's are from the legitimate and authorized companies which will also grantee the security at infrastructure level and the administrators who are creating and managing the virtual infrastructure over these equipment's are all secured. As most of the companies provide data which needs to be shared among different resource which can be located geographically apart and the developers working on these infrastructures can also be located apart it's important to maintain secure data transmission channel for sending and sharing data from different sources and from different infrastructures located geographically apart in the same organizations. The administrators not only have the task of creating the required and the best virtual infrastructure for the requesting project they are also responsible for selecting the right security path which will create virtual machines in the secured zones so that no unauthorized user can gain access to the unwanted resources residing on the same hyperconverged environments. Thus legitimate users will only be granted access to resources which they would like to share for the concerned projects on which they are working and only for a specific period of time once the project is completed and the client has been delivered with the project and the project does not have any bugs remaining to be solved then the access to the project resources will be unauthorized once the project is completed and the development team members have delivered the project to the required company.

5. ADVANTAGES OF USING SECURE HYPER-CONVERGED ARCHITECURE

As many architectures focus on security only and compromise the performance by adding high security protocols which slow down the performance of the machines. The architecture which I have proposed will improve security and the users need not comprise on performance of the systems.

A. Improve security

The architecture will improve security without compromising on the performance related aspect of utilizing the virtual machines on the virtual networks and accessing VSAN over the virtual network. This system will provide clients resource sharing and resource allocation for the projects which they are working on the clients can request for the resource from the administrators the administrators can allocate the resources remotely to the requesting clients resource sharing and allocation can be done by the administrator.

As all the equipment's which are used for designing the hyperconverged systems are from legitimate and authentic sources its reliability and authenticity will also depend on the vendors who are providing the resources for designing the hyperconverged environments. The virtualization environments from VMware are highly secure and are being used by most of the fortune companies today so if the organization is using all the legitimate resources it will be easy for the administrator to manage and create virtualized environments for the clients and the projects can be allocated resources when demanded to the administrators.

B. Availability of Resources

- The administrators can now enhance the resources of the virtual machines online without worrying about security issues over the network.
- This architecture will also reduce the latency in accessing resources over the network and improve performance of the virtual environments.
- As the resources are created on the hyperconverged infrastructure pooling of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

these resources can be done by the system administrator.

ACKNOWLEDGEMENT:

This research work would not have been completed without support of many stakeholders who have provided adequate availability of the resources on time. I would like to thank my dean Dr. Mohammed Alshehri for providing me resource on campus for completing my research work on time and for his continuous motivation and belief in my research work. Last but not the least I would like to thank all supporting staff members for helping me in all documentation work which need to be completed for procuring equipment's which were required for this research project

REFERENCES:

[1] T. Ristenpart, E. Tromer, and et al., "Hey, You, Get off My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", in CCS'09 Proc. 16th ACM Conf. on computer and communication security, pp. 199-212, November 2009.

[2] N. Cao, C. Wang, and et al., "PrivacyPreserving Multi-keyword Ranked Search over Encrypted Cloud Data", INFOCOM 2011 Proc. IEEE, pp. 829-837.

[3] Y. Zhu, H. Wang, and et al., "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds", in SAC'11 Proc. 2011 ACM Symp. on Application computing, pp. 93-102.

[4] Y. Ko. Stevn, K. G. Joen, and et al., "The HybrEx Model for Confidentiality and Privacy in Cloud computing", in 2011 HotCloud11 3rd USENIX Workshop on Hot Topic in Cloud Computing, pp. 1-5.

[5] N. L. Petroni, T. Fraser, J. Molina, and et al., "Copilot a coprocessorbased kernel runtime integrity monitor" in SSYM'04 Proc. 13th conf. on USENIX Security Symposium, pp. 13–18.

[6] M. Christodorescu, R. Salier, and et al., "Cloud Security is not(Just) Virtualization security", in CCSW'09 Proc. ACM workshop on Cloud Computing security, pp. 98-102.

[7] Sun Park; Byungrae Cha; Jongwon Kim., "Preparing and Inter-Connecting HyperConverged SmartX Boxes for IoT-Cloud Testbed", IEEE 29th International Conference on Advanced Information Networking and Applications, 2015, pp. 695 – 697

[8] Anirban Kundu; Ruma Dutta; Debajyoti Mukhopadhyay, "Converging Cellular Automata Techniques with Web Search Methods to Offer a New Way to Rank Hyperlinked Web-Pages" International Symposium on Information Technology Convergence (ISITC 2007), 2007, pp. 291-295.

[9] Carlos Melo; Jamilson Dantas; Andre Oliveira; Danilo Oliveira ; Iure Fé; Jean Araujo; Rubens Matos; Paulo Maciel., "Availability models for hyper-converged cloud computing infrastructures", Annual IEEE International Systems Conference (SysCon), 2018, pp. 1-7.

[10] Zhe Wang; Jin Zeng; Tao Lv; Bin Shi; Bo Li, "CloudAuditor: A Cloud Auditing Framework Based on Nested Virtualization", IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 50-53.

[11] Hua Cheng; Zuoning Chen; Ninghui Sun; Fangyuan Chen; Mingyang Wang, "Evaluation framework of virtualization systems for cloud computing", IEEE Asia Pacific Cloud Computing Congress (APCloudCC), 2012, pp. 48-52.

[12] Javier Prades ; Federico Silla, "A Live Demo for Showing the Benefits of Applying the Remote GPU Virtualization Technique to Cloud Computing", 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 735 – 738.

[13] Tenepalli Deepika; Appini Narayana Rao, "Active resource provision in cloud computing through virtualization", IEEE International Conference on Computational Intelligence and Computing Research, 2014 , pp. 1-4.

[14] B. Asvija; R. Eswari; M B. Bijoy, "Virtualization detection strategies and their outcomes in public clouds", IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia), 2017, pp. 45 – 48.

[15] Fatima Shakeel; Seema Sharma, "Green cloud computing: A review on efficiency of data centres and virtualization of servers", International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 1264-1267.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] Caifeng Zou; Huifang Deng; Qunye Qiu, "Design and Implementation of Hybrid Cloud Computing Architecture Based on Cloud Bus", IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, 2013, pp. 289-293

[17] E. Aruna; A.Abirami Shri; Ajanthaa Lakkshmanan, "Security concerns and risk at different levels in Cloud Computing", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 2013, pp. 743 – 746.

[18] Yicheng Zheng; Feng Deng; Qingmeng Zhu; Yong Deng, "Cloud storage and search for mass spatio-temporal data through Proxmox VE and Elasticsearch cluster", IEEE 3rd International Conference on Cloud Computing and Intelligence Systems, 2014, pp. 470 – 474.

[19] Ashalatha R.; Jayashree Agarkhed; Siddarama Patil, "Network virtualization system for security in cloud computing", 11th International Conference on Intelligent Systems and Control (ISCO), 2017, pp. 346 – 350.

[20] Valentina Salapura, "Cloud computing: Virtualization and resiliency for data center computing", IEEE 30th International Conference on Computer Design (ICCD), 2012, pp. 1-2.

[21] Chengjun Xu; Quanhong Tian; Heng Zhang, "A research of safety mechanism in cloud computing platform based on virtualization", 7th International Conference on Computer Science & Education (ICCSE), 2012, pp. 245 – 248.

[22] Poonam V. Kapse; R. C. Dharmik, "An effective approach of creation of virtual machine in cloud computing", International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 145 – 147.

[23] Seongwook Jin; Jinho Seol; Seungryoul Maeng, "Towards Assurance of Availability in Virtualized Cloud System", 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, 2013, pp. 192 – 193

[24] Guodong Zhu; Yue Yin; Ruoyan Cai; Kang Li, "Detecting Virtualization Specific Vulnerabilities in Cloud Computing Environment", IEEE 10th International Conference on Cloud Computing (CLOUD), 2017, pp. 743 – 748.

[25] Zhao-Yue;Shan-Yan. The mould research and development of virtual laboratory [J]; Light industrial machinery; 06, 2011.