Future Security of Virtualization and 3 dimensional Storage using Fog Computing and Cognitive Network

1st Mehedi Hasan
dept. of computer science and engineering
Brac University
Dhaka, Bangladesh

2nd MD.MORSHEDUL ISLAM
dept. of computer science and engineering
Brac University
Dhaka, Bangladesh

3rd Sumaiya Haque
dept. of computer science and engineering
Brac University
Dhaka, Bangladesh

***Abstract*—This paper we will discuss effective network and security virtualization, as well as storage and computing virtualization. A virtualization technique for on-demand caching functions for the forwarding process, then construct an information exchange mechanism between the two nodes which is fog and future Internet. This work effectively explains the design, numerous implementations, and assessment of Stonehenge, which is a multi-dimensional storage virtualization system that is capable of virtualizing a cluster-based storage system along several dimensions, such as bandwidth, size capacity, and latency. Also, it will provide insights into how multi-tenant virtual network ization is done on the Open Stack platform, with a special focus on performance issues, in order to fill a gap that has begun to attract the attention of the developer community. The objective of this study is to identify the NFV paradigms' cloud implementation limitations. Under an ad hoc series of tests, the performance of OpenStack in critical load scenarios was tested in single and multi-tenant environments. Different network security strategies have been presented in this article for future assaults. The security of the whole virtual network environment is enhanced by the smooth refined virtual machine control mechanisms and the entire security domain.**

I. Introduction

Although presently cloud computing is still in its infancy, it is projected to grow in popularity as time goes on. In the future, enterprise software and solutions will be cloud-based. It's no surprise that more and more organizations are turning to cloud computing because of low-cost infrastructure and high-value services. These cloud-based services' technology is delivered remotely through cloud servers. This article discusses a multi-dimensional storage virtualization system that uses nodes to reduce connection latency from the cloud to the edge, as well as cloud security and data center cloud connectivity.

Clouds abstract, pool, and share scalable resources via a network, whereas virtualization allows users to operate many virtual environments or dedicated resources from a single physical hardware system. The most widely used virtual storage systems focus on a certain feature or capability of the underlying storage. Because of this, multi-dimensional storage virtualization is quite successful. Stonehenge is commonly used to virtualize various disk subsystems due to its utilization of run-time metrics throughout the whole disk resource distribution and scheduling process. The storage solution for iSCSI is cluster-based. In terms of service quality, it ensures service quality, is supported by Measurement-based Admission Control (MBAC), and employs CVC scheduling to increase efficiency. Using the virtual disk to its full capacity is advantageous since it not only meets bandwidth requirements but also frees up actual disk space. In some cases, the management server might also act as a cluster. To gain access to the primary cloud system, it must be connected to a network that also includes the storage system. This operation, however, is postponed for an unreasonable amount of time. Ignoring this delay will need the use of Cloud nodes that are located between the main Cloud system and Edge. To develop an information-centric future Internet, a fog computing-enabled cognitive network functions virtualization approach is proposed. At this location, this fog node will be part of a cluster. Because the cloud system is now closer to the edge, the distance between them will be reduced, resulting in minimum latency. The fog nodes' caching mechanism saves previous information, and we obtain the most recent data.

While virtualization technology offers certain benefits, it also has significant drawbacks. Virtualization, no-border, and dynamic migration may raise a new set of security problems for cloud computing, implying that cloud computing participants are more vulnerable to attacks to their personal privacy, corporate interests, and even national security. We've included some additional security measures to ensure that the entire operation is secure. As a result of the combination of the virtual shift and the virtual machine monitor layer, this virtual network may surpass the traditional physical network limit. The virtual network as a whole must be effectively protected, with fine-grained management at the virtual engine and security domain levels. For access control, virtual networks employ the OpenvSwitch (OVS) technology. Virtual machine security groups may be created depending on the number of virtual machine security needs, and each group can have a set of access rules applied to it. Virtual machines are installed on distributed physical hosts and exist in security groups of the same type. Virtual machines may communicate with each other across security groups, just like they would on a real system. These cloud security solutions employ virtualized agentless anti-virus software, which prevents dangerous malware from accessing your data.

II. Overview of Fog-Computing

Fog computing is something that plays an intermediate role in Cloud and Edge Networking.Fog computing delivers services not just to communication stack, but also to the networks themselves. Network devices in IP-based network topologies do not need to perform a second resolution step to determine which fog node is closest and supply the fog node's IP address in order to communicate with one another. A traditional ICN establishes a FIB by flooding or prepopulating, The method is same as a routing table in IP-based routers, and identifies the output face of a packet in intermediary devices. For a wide-area network, this method is unsuccessful since it generates network congestion.It's a prepopulation paradigm in which all cloud users publish messages for the data they have and all nodes build the FIB based on which face they receive the announcement from. However, because the network, particularly the mobile network, changes rapidly, this technique demands that the network remain static, which implies that further and unending FIB updates will have an impact on network performance.

The FIB can be maintained and updated at the fog node since it can provide networking control functions. To address these issues,which are maintained from the original intended fog computing routing technique, may be used to dynamically control the bottom layer devices and maintain the FIB. Using Network function virtualization and software defined networking technologies, the control plane, which may be located on the fog node and forwarding devices, can be separated. This control of the ICN has been investigated, and the viability of such a scheme has been demonstrated. The Software defined networking control plane is a conceptually centralized physically distributed architecture, according to recent research.

A. *Fog Node Configuration*

The cache size of each node is set to a significant value. the prospective Internet will not be a peer-to-peer network; each network node will have its own unique characteristics, thus caching size will not be an another approach, resulting in resource waste. To increase the efficacy of caching even further, The fog node can act as a local network controller, monitoring network traffic and load while also constantly allocating caching size for future Network nodes in the region. Because most requests can be cut off and finished at the local access node, this method alleviates the problem. Furthermore, the greater the cache capacity that should be assigned to the node, the more linked it is to the end consumers. In fog computing, there is a trade-off between network performance and the cost of storage space. LRU, LFU, and FIFO are the three default cache replacement strategies in ICN. These cache rules are complicated, and they will use even more computing resources on the already-scarce information-centric Internet nodes. When a data packet is received at a node, it is first checked for a PIT match, and if it is, it is added to the content store using the caching decisions and cache management rules before being sent off. As a result, a complex caching policies, the cache policy would take a long time to run, especially in high-traffic scenarios, causing substantial processing delays.

Saving network capacity for transmission of verified data is one of the advantages of validating data packets at nodes rather than at consumers. Fog computing can be considered a suitable location for data verification without putting a strain on the network.The fog node is situated near the end user at the network edge.To simulate real-world scenarios, we compare the data store sizes of the fog node and router to the total data number in the network and suggest a substantial proportion, such as the fog node storage capacity being 500 which is 5 times the main router capacity and the total data is transferred in this network being 10,000. The client creates the incentive packet using the Zipf law at a preset frequency of roughly 100 packets/s..

III. Overview of Stonehenge-Storage

The process of integrating numerous storing devices from a single physical storage resource is referred to as ”storage virtualization.” The vast majority of storage virtualization solutions, also known as hypervisors, are focused on a single storage feature or capacity. The importance of Multi-Dimensional Storage Virtualization cannot be overstated. We need to understand virtualization since some of them can run a cluster-based physical storage system with bandwidth, capacity, and throughput. To conclude, multi-dimensional storage virtualization has the greatest influence on disk bandwidth guarantee owing to a variety of disk performance needs that may be easily transformed into bandwidth requirements. Stonehenge can be beneficial in this situation because it includes run-time measurements into every phase of the disk resource allocation and scheduling process, including admission control, latency-derived bandwidth demand computation, and disk service time prediction. Stonehenge augments a physical storage resource with a single virtual disk. It's vital to remember that evaluating Stonehenge against other storage virtualization solutions is more challenging.

A. Storage Configuration

Many companies nowadays opt to use a different type of virtualization solution that does not require downtime for system maintenance and updates. Given that all of these storage management tools focus on system setup rather than run-time disk scheduling, it's unsurprising that run-time disk scheduling receives minimal attention in these applications. They restrict the disk I/O rate rather than the disk I/O latency when it comes to Quality of Service (QoS). One of Stonehenge's main goals is to minimize disk I/O scheduling delays to real I/O rates. Stonehenge is more concerned with request latency profiling since it is critical to ensure consistent latency for each request. Stonehenge has the further benefit of reporting on the run time state of all programs at the same time, maximizing the benefits of multi threading. It also makes use of information from each application's online profiling. Because the access time to disks is dependent on the workload, online profiling is considerably more essential when it comes to storage systems. Virtual disks that use run time measurement data might change their resource reservations on a regular basis to accommodate for any potential prior-round resource overestimation. The goal of admission control at Stonehenge was to manage the predicted pattern of disk access requests. Stonehenge calculates delay and throughput using a probability distribution function to correctly reflect observed resource consumption patterns. It employs statistical multiplexing to keep track of past procedures and reduce physical scheme inventories.

A two-level disk resource scheduler is included. These are the ones:

(1) Request scheduler for Virtual Clock (VC)

(2) A scheduler for physical disks.

The virtual Clock Scheduler (CVC) is based on CSCAN and may give additional bandwidth in this case. As a result, it ensures the storage of disk bandwidth and latency. In Stonehenge, we may describe the major characteristics of a virtual disk. These are the following:

(1) Availability (A)

(2) Bandwidth(B)

(3) Capacity (C)

(4) Delays(D)

(5) Elasticity(E)

B. System Architecture of Stonehenger Storage

There are a few steps to converting a virtual disk specification.

Step 1: It transforms A, B, C, D, and E into a set of A at a time, and virtual disks cannot be duplicated.

Step 2: Stonehenge then accepts the conversion and assigns non-replicating virtual disks 1, B, C, D, and E.

Step 3: It then turns non-replicating virtual disks to replicated virtual disks and assigns them the numbers 1, B, C, D, and E.

We may ignore A in this case because it only works with B, C, D, and E. Stonehenge also assigns a single physical storage server to each virtual disk B, C, D, and E.

Data processing units, disk control arrays, and other components are found in storage servers. Reservations for virtual disks are frequently delivered at different times throughout the day. With a virtual disk, Stonehenge may be able to attain higher levels of performance and capacity than any other single physical storage server. One disk at a time is recognized using mapping heuristics, and a virtual disk may only be created when all of the component partial disks have been authorized. There are other virtual driving mirrors that may be used to satisfy this requirement.

Stonehenge is an iSCSI (Internet Small Computer Solution Interface)-based statistics storage system. It is made up of a storage manager and a number of storage server nodes connected by a Gigabit Ethernet network.

The storage manager and virtual disk specifications control the number of virtual disks that may be used and aid in meeting the QoS criteria set by the central management software. Actually, Stonehenge aids in the simplification of procedures and the optimization of server nodes.

Stonehenge's two levels of abstraction are achieved using a disk scheduler design with two degrees of abstraction.

To learn about the virtual disks, the client first connects with the storage management. It is then sent to a dedicated storage server node after processing. The server node then delivers the information to the central management system. The central management is not directly involved in the data transmission process. The virtual clock (CVC) approach, which employs a virtual clock on the central management server, is used to compute request deadlines. The sequence in which distinct virtual disk request processing is conducted to ensure that each virtual disk's QoS criteria are met is defined by an interesting approach employed here. A disk request scheduling approach enforces each virtual disk's QoS criteria, while an admission control system accepts more virtual drives. You'll also get the very efficient QoS-guaranteed Disk Scheduling feature as a free bonus.

To summarize, Stonehenge can improve its performance guarantee and system use efficiency while still maintaining the greatest performance guarantee and usage efficiency. Furthermore, Stonehenge enables for the inclusion of more virtual disks in the total storage system. With QoS-Guaranteed Disk Scheduling, this device is also highly efficient. Let's say that multi-dimensional storage virtualization is done at Stonehenge, and that it entails a number of ways for achieving this aim while keeping costs to a low.

IV. Overview of OpenStack Platform

OpenStack offers cloud administrators with a web-based interface as well as a sophisticated and adaptable (API) for controlling a group of physical hosting servers that use various Hypervisors.

The controller node, network node, computing nodes, storage nodes, management network, tunnel network, and external network make up Openstack. An OpenStack lodger is a virtual infrastructure in the cloud that may be created by creating a whole new network and then connecting it to its parent network. Neutron establishes a port on each of the subnet and connects the VM to the principal network of that subnet, while the (DHCP) service on that network assigns the VM a secure IP address. Other virtual programs (such as routers, which require global connection) can be run directly in the Cloud platform utilizing containers and other network namespaces, which are often established in the entire network node. A graphical tools that was created to display all of the various network components that are often utilized by OpenStack. Two instances of the internal state of a network node connecting to three different virtual subnets and a compute node running two virtual machines. VLANs, which are layer 2-in-layer 3/4 digging solutions, or Generic Routing Encapsulation can be used to provide layer 2 virtualization as well as multi-tenant isolation on the primary physical network (GRE). The compute node that will host the VM is chosen by the OpenStack scheduler component running on the controller node.

In an OpenStack system node, network components are linked to three distinct virtual subnetworks. The test cases were created in accordance with OpenStack's design. The OpenStack Dashboard view used to generate the numerical results presented below in the situation of four tenants running at the same time. The selection of four workers was made without regard for generality in order to provide substantial results of acceptable complexity. As the findings demonstrate, it is completely sufficient to put the compute node's hardware assets under stress, therefore evaluating performance limitations and significant concerns.

V. Exploring Security of Stonehenge Storage and Node

The virtualized network's dynamic boundary characteristic causes extra challenges for the fixed-bound network security control technique as compared to traditional physical networks. By placing the device on a well-defined network border, traditional physical devices allow network traffic to be limited and monitored. However, the VM are primarily connected via the VS and VI supplied by the virtual monitor coating, allowing the virtual network to connect to the regular physical network. Some approaches for various issues are presented in this work.

A. Security Architecture

1) Access Control for Virtual Networks is a mechanism based on the Open vSwitch (OVS) that may be used to restrict access to whole virtual networks. The technology's generic security agent mode allows access control over data packets flowing in and out through a number of various channels. This agent mode may perform a variety of tasks, including security control optimization, synchronization, and many more.
2) Virtual Machine Access Control is in between the virtual machines; there are two distinct requirements for contact: the first is when an individual virtual machine links with other individuals who live on comparable hosts, and the second is that they both reside on discrete hosts. On the virtual ports or virtual switches that may implement the entire access control mechanism, a security assessment of the safety domain or vLAN for such kind of virtual computers is listed, along with the total control rules.

3) Dynamic Migration for the Entire Security Policies refers to the dynamic changes in the virtual machine, as well as the dynamic changes in the entire virtual network, which can make security deployment and maintenance extremely difficult, as well as putting such security measures at risk of failure. The virtual network safety system's dynamic security migration function ensures that the proper security policy is consistent in the face of dynamic virtual machine shifts and dynamic virtual network changes. With the virtual machine management interface, the security officer's bands may keep track of the aforementioned shift status and changes in network setup. To maintain a stable security policy before and after a change, the Security Center will centrally bring up the security policy source as well as the detailed network security policy on the main target virtual machine that primarily changes, and then all updated records will be forwarded to that specific virtual machine's network control point.
4) Virtual Network Traffic Monitoring, as well as physical network traffic, may be completely monitored in the whole cloud computing information center, as opposed to traditional network traffic monitoring. Unlike traditional Cloud security monitoring systems, customers may now attempt to regulate the whole operating condition from a global viewpoint by focusing on the operational state of all cloud data centers
5) The whole network traffic monitoring and analysis component is in charge of all-encompassing as well as multi-grained and multi-layered collection, analysis, and pulling out of both virtual and physical network traffic. It can typically recognize multiple apps properly based on the built-in acknowledgement. It can also create total relation maps on the fly to assist users in mastering the real-time connection between application services running throughout the whole internal virtual network.
6)The virtual nodes, networks, and storage are all monitored by the operational status monitoring system, which looks at how well they're being used.. The many sorts of dimensions, such as time, category, matrix, and the structure of multiple virtual ports, may all be readily customized by users. It basically checks the overall capacity allocation, as well as the utilization factor and throughput rate, for various virtual storage.
7)Virtualized Agents as an Anti-Virus Mechanism By imple-

menting virtualized agentless anti-virus software in data centers, cloud security solutions often prevent virus imposition. To prevent data theft and harmful assaults from other virtual machines, Hypervisor can identify the isolation between various virtual machines residing on the same physical host. End users can only access their own resources, such as hardware, software, and data, and they can't access the resources of others..

8) According to the traffic diversion solution, in order to achieve basic isolation and various sophisticated safety features such as IPS and Layer 4 to Layer 7 antivirus, the typical VEPA traffic diversion technique includes the imperceptible flow in the secondary layer, which is vSwitch in physical safety devices. It also keeps the network and server administration under control by efficiently discharging all of the host resources.

VI. Methodology Performance Evaluation

We have learned from the above methodological talks that virtualization in storage, network, and security can be done more quickly and efficiently. Our articles explained the components and procedures utilized in the systems and provided us a clear picture of them. We were able to connect our articles, and we believe that our new concept will be beneficial for future study and development. In our papers, it can be observed that we use nodes for networking and Stonehenge for storage. Some of our principles have been utilized in previous studies, but our data show that our technique is significantly quicker and more efficient. When it comes to storage virtualization, Stonehenge is clearly distinguished from local storage systems. Stonehenge has a fixed amount of disk space. On QoS metrics, there is a lower delay bound. It makes use of the CVC Scheduler, which may provide free bandwidth according to the reservation of the participating virtual disk. It is more concerned with request delay profiling. During admission control, it adjusts resource reserves based on run-time measurement input. It also keeps track of probability distribution functions to summarize the observed latency and throughput resource consumption trends. Stonehenge, in comparison to other storage virtualization systems, can virtualize a storage resource in several dimensions. It's an iSCSi storage system with a cluster. Even the management server may function as a cluster. The criteria for admission control is bandwidth. It helps to reduce resource waste due to over-provisioning and gathers workload information more precisely at run time than others. It transforms bandwidth reservation to delay bound. It allows users to easily utilize the virtual drive while still meeting bandwidth constraints. So, in general, Stonehenge is superior since it concurrently meets all bandwidth needs, takes less time to run, has better CVC and QoS guarantees, is more effectively admission managed, and is multidimensionally virtualized. One disadvantage is that Stonehenge does not use a load balancing technique. We took use of this flaw to develop a more efficient method of storing data, which was later included in the OpenStack platform. In comparison to fog computing and the OpenStack platform, where both nodes are utilized for network functions, we are now employed to receive the stored data. Nodes aid in memory caching and data recognition, allowing us to access information more quickly. Data is immediately retrieved from the cloud by an EDGE user, resulting in significantly reduced latency. This is the fastest way to receive data from the cloud. We should also be worried about network security while doing all of this fancy computing and networking. For various scenarios, several methods for network security have been introduced. Among all the security measures, we believe network traffic monitoring and traffic diversion solutions will be beneficial to the user, according to our study. The solutions not only provide us with security, but they also improve the performance of our virtual networks.

VII. Conclusion

In this paper, we study that Stonehenge Storage and Cognitive Caching Cloud Along with OpenStack Provides the best way to retrieve data from the Cloud. It also Provides the best security to the Cloud System and the Edge User. Though some of the challenges also exist, we can ignore that.As the security of these methods is much higher and also it provides much faster data because of the cognitive network and Nodes Caching Policy. Users can Retrieve the data much faster which is our main concern and also it provides best security to the user to protect their data.

References

[1] Sun, Junjun Zeng, Ying Shi, Guowei Li, Wei Li, Zhihong. (2018). The Research for Virtualization Network Security on Cloud Computing. 10.2991/icaita-18.2018.37.

[2] Wu et al., "FCSS: Fog-Computing-Based Content-Aware Filtering for Security Services in Information-Centric Social Networks," IEEE Trans. Emerging Topics in Computing, pp. 1–12. DOI: 10.1109/TETC.2017.2747158, 2017.

[3] J. Wu, M. Dong, K. Ota, J. Li, W. Yang and M. Wang, "Fog-Computing-Enabled Cognitive Network Function Virtualization for an Information-Centric Future Internet," in IEEE Communications Magazine, vol. 57, no. 7, pp. 48-54, July 2019, doi: 10.1109/MCOM.2019.1800778.

[4] Lan Huang, Gang Peng, and Tzi-cker Chiueh. 2004. Multi-dimensional storage virtualization. SIGMETRICS Perform. Eval. Rev. 32, 1 (June 2004), 14–24. DOI:https://doi.org/10.1145/1012888.1005692

[5] A. Singh, M. Korupolu and D. Mohapatra, "Server-storage virtualization: Integration and load balancing in data centers," SC '08: Proceedings of the 2008 ACM/IEEE Conference on Supercomputing, 2008, pp. 1-12, doi: 10.1109/SC.2008.5222625.

[6] A. Ma, Y. Yin, W. Na, X. Meng, Q. Bu and L. Xu, "Scrubbing in Storage Virtualization Platform for Long-Term Backup Application," 2009 International Conference on Availability, Reliability and Security, 2009, pp. 441-447, doi: 10.1109/ARES.2009.87.

[7] C. Zhang, M. Dong and K. Ota, "Fine-Grained Management in 5G: DQL Based Intelligent Resource Allocation for Network Function Virtualization in C-RAN," in IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 2, pp. 428-435, June 2020, doi: 10.1109/TCCN.2020.2982886.

[8] Franco Callegati, Walter Cerroni, Chiara Contoli, "Virtual Networking Performance in OpenStack Platform for Network Function Virtualization", Journal of Electrical and Computer Engineering, vol. 2016, Article ID 5249421, 15 pages, 2016. https://doi.org/10.1155/2016/5249421

[9] Ahmed, J., Malik, A., Ilyas, M.U. et al. Instance launch-time analysis of OpenStack virtualization technologies with control plane network errors. Computing 101, 989–1014 (2019). https://doi.org/10.1007/s00607-018-0626-5

[10] Sun, Junjun Zeng, Ying Shi, Guowei Li, Wei Li, Zhihong. (2018). The Research for Virtualization Network Security on Cloud Computing. 10.2991/icaita-18.2018.37.

[11] . Chaudhary, N. Kumar and S. Zeadally, ”Network Service Chaining in Fog and Cloud Computing for the 5G Environment: Data Management and Security Challenges,” in IEEE Communications Magazine, vol. 55, no. 11, pp. 114-122, Nov. 2017, doi: 10.1109/MCOM.2017.1700102.