Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Design and Implementation of Out-of-band Storage Virtualization

Nikita Jain (Parkha)
Research Scholar
Dept. of Computer Science & Engg.
Kalinga University, Naya Raipur
Chhattisgarh, India

Ms Sana Tak
Asst. Professor
Dept. of Computer Science & Engg.
Kalinga University, Naya Raipur
Chhattisgarh, India

***Abstract*—Storage virtualization is the most applied word in the industry due to its importance. Now a day's data become more import, to hold and to extract needful information. Datacenter become an integral part of any organization, so its management too. For best and efficient result as well as proper storage utilization and management we need storage area network (SAN). In the environment of SAN, there is the compatibility issue with the different vendors and their drivers, so we are going for storage virtualization. Storage virtualization is applied in SAN environment. The classical techniques! 1] to achieve storage virtualization is suffering from many problems like improper disk utilization, high latency, power consumption, different attacks and security issues. In this paper we design and implement storage virtualization technique EC2S2 to get. better yield in terms of security, high throughput, efficient management and least latency. Through the security and performance analysis we show that our method is secure and efficient.**

Keywords— Storage, Virtualization, Out-Of-Band, Security, Thin-Provisioning, Power Management, Memory Management.

I. INTRODUCTION

Storage virtualization is the one of virtualization technique which abstracts physical storage and creates pool of logical storage. These physical storages might be scattered and connected through some storage network. The main goal of developing storage virtualization is for flexibility, scalability, efficiency, manageability, availability and disaster recovery. The main architecture of storage network consists of storage, network devices and host.

The definition of storage virtualization according to SNIA[ll] is as 'The application of virtualization to storage services or devices for the purpose of aggregating functions or devices, hiding complexity, or adding new capabilities to lower level storage resources."

The storage virtualization can be achieved at different level with different strategy. The virtualization may be file level or block level. Infrastructure wise the virtualization may be host base, storage based or network-based approach. Depending Upon how data and control flows, In-band and Out-of-band storage virtualization can be achieved. When data and control flows through the same channel it is in-band whereas different channel is involved it is out-of-band. The storage virtualization is mainly of block level, which facilitates computer to access storage as a normal physical drive. The main advantage of storage virtualization is to reduce implementation cost, maintenance cost and increasing efficiency. The storage virtualization provides better resource utilization. Policy based resource allocation can also be possible which ensures Quality of service in storage Virtualization.

Based on the study made by Zhang et al.[2] and Benard Mwathi [8], there are several severe problems which should be addressed. In the storage virtualization, disk is not utilized properly. Some of network controller which are not much of high frequency, they impart high latency. Since virtualization is a technique where a large mainframe computer resource is shared among various VMs through the help of hypervisor which is a software program that provide a layer between host and guest machine, so it has all trivial software issue and vulnerabilities as well as some other faults. In the virtualization technology, the security requirement is very high because there are more number of logical machines and more risk of entry points, holes and interconnection point that are more vulnerable to attacks.

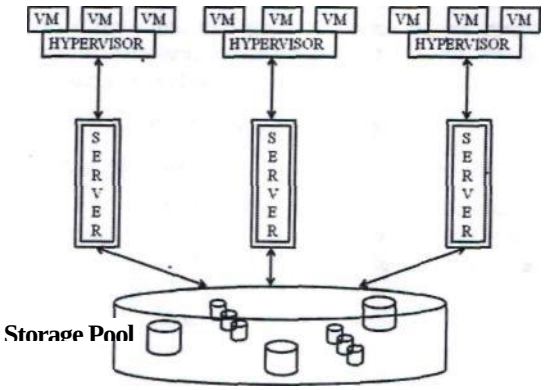

Fig 1: Basic Architecture of Storage Virtualization

Fig. l shows the basic architecture of general storage virtualization architecture. This architecture is consisting of a pool of different storage devices which is policy based allocated to VMs ruled by hypervisor installed on respective server. This is the native architecture of storage virtualization.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Recently, some researchers designed storage virtualization in different ways. However, none of them are efficient, secure and providing traditional issues solution. In this paper, we proposed an efficient and secure design of storage virtualization by employing cryptographic technique through file manager and drivers with minimal hardware support. The use of thin provisioning to get better and efficient storage utilization along with multiprotocol switch that is useful for reducing latency and power requirement while accessing the SAN. Through the security and performance analysis, we show that our method is secure and efficient.

II. RELATED WORKS

Virtualization is the key technology that empowers cloud computing. Cloud is essential because local resource is limited and not consistent across multiple devices. Storage virtualization is an example of resource virtualization which creates a pool of logical storage by abstracting all physical resource. Some of the researchers have designed storage virtualization recently.

Study on memory management approach in virtual environment by xian chen et al.[4] has revealed many things like page sharing which was mostly implemented by self-sharing whose rate varies between platforms. Page size has also significant influence on Linux than windows platform. They have given very nice approach to manage memory by the study on different OS and page sharing concept, but this approach was not solving the disaster recovery issue efficiently.

Xiaojia xiang et al.[5] found the necessity of redundant hardware and software as well, so they proposed the inclusion of remote mirror that will keep information system active all the time even during site corruption. This approach is much focused on redundancy of hardware and software to facilitates disaster management but still inefficient to provide security.

AhmedA. Faris et al. [6] finding on storage performance in virtualized environment • that there are interface queue saturation when storage system becomes busier. Such misconfiguration may impact performance issues. They have targeted the storage content which was underutilized. They have pointed out the relation between the performance and fraction of utilized storage. They didn't included security in his technique.

The study made by Jae woo choi[7] to make high performance SAN. They tried DRAM based SSD, but the latency was high even with high speed networks were used. So his finding was to remove software overhead in SAN I/O path, increasing parallelism in the handling of I/O request along with temporal merge mechanism. This technique has some compatibility issue between the storage vendors.

III. PROBLEM STATEMENT , I

A. Problem Definition

In the study of storage virtualization, we found that storage virtualization system has four major and serious issues that should be solved to get a better and efficient system, those are

1. Security,
2. Memory management,
3. Power management and
4. Disaster Recovery.

All these problems are related with service provider and service user in different ways.

B. Threats

There are mainly two types of attacks are possible viz. Resource attack and Data attack. Resource attack may take place against cloud provider or service provider. Data attack, it may happen against service provider along with service users.

C. Goals

We designed an efficient and secure storage virtualization to achieve the following goals.

1. Security issue related with storage virtualization is major part of our work. The main idea behind security is to provide isolation among VMs must be guaranteed. If there is any flaw in isolation, one application running in one VM can access data in different one. and may capture or infect other VMs. Such scenario will impact the goodwill of service provider. Isolation must be there in such a way that VMs should be unaffected by another one which is totally affected in some way.
2. Next thing of security is the proper implementation of hypervisor enables us to protect against all kinds of software issues because hypervisor is just a software implemented layer over the server. This hypervisor layer provides support for virtualization in storage area network. So, all kinds of responsibilities come here.
3. Memory management is also challenging task here to consider. In storage virtualization we have plenty of storage pool out of which we are consuming a small amount of storage. This kind of storage utilization remains a lot of voids and unused space in the storage device. Such underutilized space must be monitored and managed to yield high throughput. We can keep track of such space by the Bit-map technique, this technique consumes very little amount of memory to run this service. We can get high throughput by increasing Parallelism as well as by removing unnecessary software overhead. Along with all these concepts thin provisioning is the technique that applies to large scale storage area networks which allows space to be easily allocated to the server on Just-in-time basis. If it is not managed, denial of service may occur.
4. Power management plays a critical role in the determination of how much system is eco-friendly. The power consumption of the system defines its efficiency as well as economical ability. Power consumption depends' mainly on the architecture of the system, software and operating system settings. To overcome this problem, we should go for multiprotocol switch which regulates the system properly and efficiently.
5. Sometimes due to unavoidable circumstances system may not response for the client request. In such instances, service provider may not able to satisfy the requests. The major challenging part of any storage services is that it should be available and recoverable. The major downtime at the time of disaster should be managed properly by various techniques. For this purpose, we must have redundant amount of hardware and software infrastructure to facilitate disaster recovery. RAID and Mirroring takes a challenging role in the creation of such an efficient infrastructure. During downtime of the service, the request must be diverted to the disaster recovery site. This is very essential part of storage virtualization.

IV. PROPOSED METHOD

To address all the issues under consideration, <we propose Enhanced Cloud Control and Security System (EC2S2) which is secure and efficient implementation of out-of-band storage virtualization, which is targeted to provide security to the storage virtualization as well as proper storage and power

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

management for enhanced and efficient kind of infrastructure. Our method provides proper isolation and integrity to the VM's in the storage area network under virtualization technology. This method employs cryptographic technology used by the file manager and assisted by minimal hardware support. The method is incorporated with the cryptographic technique that ensures the session-based access and cross verification of the identity of the access request. The use of Thin-store [9] ensures the disk utilization in the environment of storage area network where a pool of storage management of unutilized sectors are poorly implemented Secure Storage Virtualization

1. Thin Provisioning
2. Multiprotocol Switch

A. Secure Storage Virtualization

Our system allows secure access control to the storage virtualization approach. The security is enabled by adding file server, Client component and SAN component [8]. These security components are based on cryptographic capabilities issued by file manager and verified by drivers with least hardware support. This technique provides secure communication link and allows encryption of data using SSL. This framework works as follows.

1. The request is made by VMs for a file.
2. File server generates (Token+Path) and passed to Client component.
3. The Client component and SAN component establish a session using asymmetric key cryptography. After establishing the session, component server continues communication using symmetric key encryption. Once the session expires, each of the system denies the symmetric key used for that session.
4. Client component encrypts the token used in the session establishing phase. This encrypted token along with encrypted(Token+Path) is passed to hypervisor.
5. VM passes E(Token+Path) to SAN component.
6. The token is validated and authenticated by SAN component.
7. If token validation is successful then storage network is allowed to release file or operation will be denied.
8. Once storage network is allowed, the file will be made available to the VM.

B. Architecture of Thin store.

The technology of thin provisioning is based on Thin store[9]. Thin store component of the proposed method comprises of four parts.

1. Metadata Manager
2. Address Mapper
3. Storage Reclaimer
4. Resource Monitor

Metadata Manager: The metadata manager plays a pivotal role in the management of metadata which is essential for virtualization and controls logical volume and mapping table. *Address Manager :* It is mainly aimed for load balancing and processes mapping request from logical volume. It dynamically allocates physical address from the storage. *Storage Reclaimer:* Its responsibility is to manage free space. This helps thin provisioning an efficient approach to utilize storage in the better manner.

Resource Monitor: It looks into the state of storage device and manages the storage spaces when its total capacity is about to finish.

C. Multiprotocol Switch.

This switch is mainly employed due to making of an energy and latency efficient. The energy requirement of physical and control plane switch is very less as compared with the conventional Ethernet router. In this switching system, switch interface only sends and receives the multiprotocol packets in the PCIe signal format. The architecture of this switching system is based on CSMA-ST(Space Time-CSMA). This approach elevates switching capacity by improving transmission speed of CSMA-CD. The data and control of the switch are basically managed by two similar switch board which are kept at the both end of Switch Access Card (SAC) inside the switching architecture.. This approach provides more flexibility and more switching capacity due to separation of the data and control signal.

V. SECURITY ANALYSIS

In security analysis, we analyze the security of our method. The security level of our proposed method is very secure. There are several security issues are present in the existing solution.

1. Isolation
2. Application Security
3. Computing Security
4. Data Security

Isolation: The virtualization depends on the hypervisor, so the responsibility of hypervisor is a major role in the management of VMs. The cryptographic technique incorporated with the existing hypervisor enables isolation of VMs. *Application Security:* Thin store, based on thin provisioning manages the storage, maps logical address with the physical address as well as utilizes the unclaimed storage. *Computing Security:* Uses of Multiprotocol switch and cross validation of the token helps to get the computing security. *Data Security:* Once the token is authenticated then only VMs are allowed to access the storage device. In this way it ensures the data security.

The analysis based on the security aspects credits our system very high because the session based token used with different cryptographic technique helps very much in ensuring the identification, authentication as well as authorization.

VII. CONCLUSION

In this paper, we presented a design and implementation of storage virtualization with security and efficiency. The mechanism includes thin provisioning, inclusion of multiprotocol switch along with cryptographic technique. Using the proposed method, one can achieve energy efficient and low latent storage virtual ized environment. The use of thin provisioning advances the system to achieve better disk utilization and the multiprotocol switch makes the system energy efficient as well as cryptographic technique makes it secure. Security analysis of this method shows this as secure method over previous one due to time session based token passing mechanism, which ensures the access only when the valid token is received for that session else rejected.

We assume that this method provides sufficient advancement over the existing systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

III. REFERENCES

[1] Li Bigang, Shu Jiwu, Zheng Weimin, "Design and Implementation of a Storage Virtualization System on SCSI Target Simulator in SAN", Tsinghua Science and Technology ISSN 1007-0214 17/18 pp 122-127 Volume 10, Number 10, February 2005.

[2] Guangyan Zhang, Jiwu shu, Wei Xue and Weimin Zheng, "Design and Implementation of an Out-of-Band Virtualization System for Large SANs", IEEE Transaction on computers, Vol 56, No 12, Dec 2007.

[3] Jiang Guo-song, He Xiao-ling, "Design and implementation of iSCSI Out-of-band storage virtualization", 2011 International Conference on Intelligence Science and Information Engineering.

[4] Xian Chen, Wenzhi Chen, Peng Long, Zhongyong Lu, Zonghui Wang, "SEMMA: Secure Efficient Memory Management Approach in Virtual" 2013 International Conference on Advanced Cloud and Big Data.

[5] Xiaojia Xiang, Hongliang Yu, Jiwu shu, "Storage Virtualization Based Asynchronous Remaote Mirror', 2009 Eight International Conference on Grid and Cooperative Computing.

[6] Ahmed. A. Faris, Mohamed. A. Shrud, Ahmad. H. Kharaz, "Towards an Efficacious Storage Performance in Virtualised Environment", 2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems

[7] Jae Woo Choi, Dong In Shin, Young Jin Yu, Hyeonsang Eom, Heon Young Yeom, "Towards High-Performance SAN with Fast Storage Devices", ACM Transactions on Storage, Vol. 10, No. 2, Article 5, March 2014.

[8] Benard O. Osero, David G. Mwathi, "Implementating Security on virtualized network storage environment', International journal of Education and Research, Vol. 2 No. 4 April 2014.

[9] Kai Qian, Letian Yi, Jiwu Shu, "ThinStore: Out-of-Band Virtualization with Thin Provisioning" 2011 Sixth IEEE International Conference on Networking,' Architecture, and Storage.

[10] Haojun Luo, Joseph Y.Hui, Ayman G. Fayoumi,"A Low Power and Delay Multi-Protocol Switch with IO and Network Virtuahzation", 2013 IEEE 14th International Conference on High Performance Switching and Routing.

[11] www.snia.org