Protection of Data Assets in Cloud Environment with Virtualization as a Service

Shelly[1],
[1]M.Tech Department of C.F.I.S,
GITAM, MDU Rohtak

Ashish Kumar Sharma[2]
[2]Assistant Professor
Department of Computer Science And Engineering
C.F.I.S, GITAM, MDU Rohtak

Cloud and virtualization are different term, as per NIST Cloud Computing standards- Cloud provide 'VaaS' (Virtualization as a Service) to all third parties for cost effective and time shaving model and virtualization is a term used to share the same hardware resource for different services as hypervisor. Resource and hardware sharing influence the problem of data reliability, security, privacy, thefts and impacts on other legal or inter actual right acts. Data protection is carried out by implementing uniquely identified sandboxes 'UIS' wrapped with virtualization technology 'VT' in cloud environment for hardening cloud security in real-time. Primary focusing on the stand-alone sandbox's encryption over hardware with real-time decryption mechanism as the part of physical defenses. Given problem solution for crown jewel data or data assets increments the interest of organizations toward the reliability of cloud computing technology. This solution will be going to optimize response time, integrity, reduce replication, prevent data leakage, proper data distribution and latency, cost effective model. The traditional solution is lacking in some of the areas like data reliability, leakage and stealing example of icloud hacks.

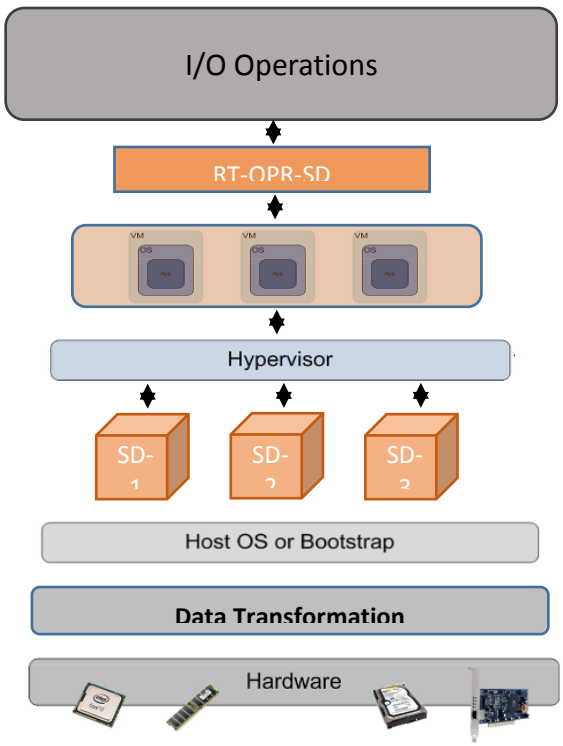
Index terms – Data Protection, Virtualization, VM, Sand Box.

I. INTRODUCTION

This Paper mainly focused for securing the risk of data leakage and help to increase son the cyber security alliances. Cloud computing technology provide lot of features for computer computation but only because of improper lack of cloud security impact on the use of this technology. Our proposed solution for data leakage prevention or other data related solution is mainly focused on protection of data based on specialized subject lines. Our solution is consisting of cost effective, data transformation, different data operation and isolation operations for data protection without any white list or old mechanism rule base solutions. As per our approach, we follow different integrals phases with pre-defined process steps for performing data operations in cloud environment for preventing data hazards.

II. METHODS AND PROCEDURES

Our approach consists of hypervisor solution provided in virtualization security for distribution of tasks and services for different virtual environments. Data classification mechanisms for data distribution is carried out by some data leakage prevention (DLP) technology. Data isolation mechanisms for data separation based on AAA, Risk, CIA and others is processed by some similar technology as presented sandbox operation solutions. Data transformation includes data encryption, data decryption, data compression/decompression, data encode/decode or other data operations is carried out in 2-ways in which one is forreal-time operation for primary memory and other is for storing hard data to secondary memory. Our main aim is to protect the data while not going to impact on quality of services like response time, user



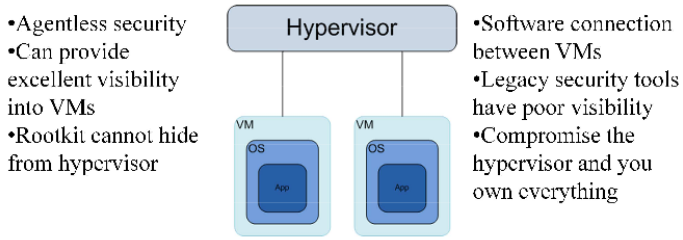
friendly and other features required for good IT environment and software.

The overall procedures include complete lifecycle of data operation in the most secure manner:
Input/ output operation is the user interaction level/layer from where users directly interacting the other secure layer for communication. The problem solution consists of random and separated real time generation of sandbox for current process task. Every process/task using separated sandbox for completing their operation and after completion of process operation autodestructing sandbox is process for that separated virtual machine 'VM'. This

logical process protects the data to communicate with another process without administration permission and it too protect from data tampering in real-time with another process or protect from process injection type of cyber security threats. This paper discusses about the virtual machines and virtual machine process never interact with another virtual machine process directly for this process they must reach level 3 at hypervisor where multi VM communicate with each other in highly secure manner.

At, Level 2 every VM's interacting with the sandboxes for process services or resources. VM's can share the resources only of its VM environments but as exception they also can interact with another VM's or multi VM's while reaching to another deeper secure level. This process of random generation of sandboxes is used to protect breakdown or exploitation of sandboxes from external threats randomization help to unpattern the unique identified ID for sandbox and prevent from exploitation.

At, Level 3…it's a bridge for providing actual hardware or primary operating system resources for VM's operations. In a legacy network, some semblance of an air gap exists between operating systems. For example, two systems connected to the same Ethernet network can only communicate with each example two systems connected to the same Ethernet network can only communicate with each other via the Ethernet network. If that network is disconnected or firewalled, the systems will be unable to communicate with each other In a virtualized environment however, the hypervisor always creates a software connection between systems. There is no way to completely isolate one operating system from another, without migrating one of the operating systems to a different hardware platform. It is this persistent software connection that has lead many to feel that virtualization can never be configured as securely as a legacy network.



The above slide shows some of the security gains and losses experienced when moving to virtualization. The trick is to leverage the new capabilities to augment the deficiencies. virtualization.

The above slide shows one of the potential security issues that can occur when storage resources are shared. Remember that in a IaaS environment each VM is typically stored as a single file. As are shared. Remember that in a IaaS environment each VM is typically stored as a single file. As storage requirements change, those files may be resized. Reducing the size of one partition and increasing the size of another creates the possibility that sectors containing deleted file information will effectively move from one VM to another. This could permit the owner of the second VM to recover file information stored as part of the first VM. Again, dedicating physical storage ensure that this issue does not surface. Another possible solution is to encrypt all file information stored to disk. If encrypted, moved sectors would be unreadable without the appropriate key(s).

At level 4, we use distrusted sandboxes for load balancing as we use tones of data transfers inform in plain transformation. These SD's direct interacting with main operating system for resource sharing and resource operation.

At level 5, data transformation process is carried out it includes all the data operation like encryptions, decryptions, compression, decompression, encoding. Decoding. Here all the data stored in completely unreadable to hardware for protecting from the physical security threats.

III. CONCLUSION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

ACKNOWLEDGMENT

I am very grateful to Mr. Ashish Kumar Sharma, Assistant Professor, for his support to write this paper .
I am very thankful to Dr. Neetu Sharma the head of department of computer science in Ganga Insititute of technology and management for her motivation and support during the paper.

REFERENCES

[1] Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.
[2] Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.
[3] Dealey, C. "Cloud Computing Working Group", Network Centric Operations Industry Consortium - NCOIC, 2013
[4] Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". Technology Review. MIT. Retrieved 31 July 2013.
[5] White, J.E. "Network Specifications for Remote Job Entry and Remote Job Output Retrieval at UCSB". tools.ietf.org. Retrieved 2016-03-21.
[6] July, 1993 meeting report from the IP over ATM working group of the IETF". CH: Switch. Retrieved 2010-08-22.
[7] Kyriazis, D; A Menychtas; G Kousiouris; K Oberle; T Voith; M Boniface; E Oliveros; T Cucinotta; S Berger (November 2010). "A Real-time Service Oriented Infrastructure". International Conference on Real-Time and Embedded Systems (RTES 2010). Singapore.
[8] Windows Azure General Availability". The Official Microsoft Blog. Microsoft. 2010-02-01. Retrieved 2015-05-03.
[9] Skala, Karolj; Davidović, Davor; Afgan, Enis; Sović, Ivan; Šojat, Zorislav (2015-12-31). "Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing". Open Journal of Cloud Computing. RobPub. 2 (1): 16–24. ISSN 2199-1987.