A SECURITY MECHANISM IN CLOUD ENVIRONMENT TO MIGRATE THE USER APP'S FROM NON-SECURE CLOUD TO SECURE-CLOUD BY USING HYPERV PHENOMENON

[1]Ms. R. Poorvadevi, [2]Ms. G. Suprajadevi
[1]*Assistant Professor, Dept of CSE, SCSVMV University, India*
, [2]*PG Student, Dept of CSE, SCSVMV University, India*
poorvadevi@gmail.com[1],Subrajadevi2@gmail.com [2]

***ABSTRACT*- An era of cloud computing is providing incredible amount of services or resources to the web clients requested from anywhere in the globe. Nowadays, people are majorly doing all their activities through web. No one is ready to spend more amounts of time and effort for completing their tasks. So, everybody heavily depends on some vendors or service providers. Accessing and consuming the services is not a main factor. How far the services are reliable in a secured manner. Clients are in need of protecting all the transactions and services on the cloud. We must know what kind of security issues is mainly present into a cloud environment. The major foundation of cloud security and privacy is control over the virtual machine and its functions before, preventing the malicious in virtual machine we need to analyze the hypervisor capabilities. Even though, hypervisor is a controller between hardware level applications and user application, Hypervisor will not provide the security for running huge user applications on guest platforms in cloud, when the users are running various process/applications on guest OS hypervisor will give the controlling notes or components, system configure and adaptation tools only. However, hypervisor will not have a focal point about security and need to be concerned about the possible factors for an applications which are consecutively executing on the guest OS. So, this proposed model helps to maintain all the confidential details data and services through the hytrust data control via fuzzy functions.**

Key words: Hypervisor, Hyper-V, Guest OS, Host OS, Kernel, CSP, virtual machine monitor (VMM), Cloud vendor, VMware.

1. INTRODUCTION

Cloud computing is a simple technology that has been around for a while and almost all of us have used without even knowing. In simple terms, cloud computing entails running computer/network applications that are on

other people's servers using a simple user interface or application format. It's that simple. The services of cloud computing are infrastructure as a service, platform as a Service, software as a service. Where IAAS is the most basic and each higher model abstracts from the details of the lower models. Other key components in anything as a service such as Strategy-as-a-Service, Collaboration-as-a-Service, Business Process-as-a-Service, Database-as-a-Service, network as a service (NAAS) and communication as a service (CAAS) were officially included by ITU

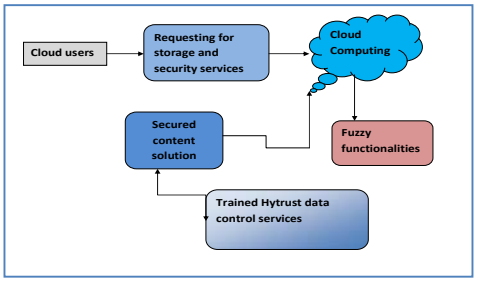
International Telecommunication Union (ITU) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem. Cloud components: client computers, distributed servers, datacenter, user data, Input request, customer service type, Offering mode, delivery recipients.

An era of Cloud architectures on the major part of virtualization concept. In this the main core component is the HYPERVISOR, which is having the key role in the virtualized environment. Even though we have a new concept is No-Hype architecture that will not provide the feasible security solutions to the end users.

1. RELATED WORK

VMware upgrades VMware Tools frequently to support new devices and to add enhancements that improve the performance of your virtual machines. When you upgrade VMware Fusion, you should also upgrade VMware Tools. VMware Journey Highlights. The following pages outline adoption highlights in aggregate, as well by key metrics , Modernization of Business-Critical Applications Pays Off Organizations are benefiting from virtual zing mission-critical business applications, which include production databases, financial systems and customer-facing. Hyper-V is the hypervisor-based virtualization technology from Microsoft that is integrated into all Dell supported Windows Server 2008 x64 Editions operating systems. As a virtualization solution, Hyper-V allows users to take maximum advantage of server hardware by providing the capability to run multiple operating systems (on virtual machines) on single physical server applications.

Fig: 1. (a) SYSTEM ARCHITECTURE



The CART (Classification and Regression Tree) is an algorithm is structured as a sequence of questions, the answers to

which determine what the next question, if any depends on user deployed application. The result of these questions is a tree like structure where the ends are terminal nodes at which point there are no more questions. A simple example of a decision tree is as follows:

The following questions are classified and Queries raised while an application deployment by the user.

a) User requirements and service types must be analyzed thoroughly.
b) Determine the suitable cloud vendor by the user request.
c) If it is needed, to know the available status of data owner (DOG) group and its services.
d) Know the functionality and limitation of virtual machine.
e) Per physical machine how many virtual machines are able to create by the customers.
f) Hypervisor control can be migrating from bar-Mattel os to user windows os.

The main elements of CART (and any decision tree algorithm) are:

- Rules for splitting data at a node based on the value of one variable;
- Stopping rules for deciding when a branch is terminal and can be split no more; and
- Finally, a prediction for the target variable in each terminal node.

Decision tree learning uses a decision tree as a predictive model which maps observations (cloud functions) and user
application deployment about security to conclude the customers target value. It is one of the predictive modeling approaches used in statistics, data mining and machine learning. From this technique, we can able to predicate what type of applications are frequently used /deploy on the virtual machine. So, more descriptive names for such tree models are classification trees or regression trees. In these tree structures, leaves represent class labels for users and branches represent conjunctions of features about hardware level that lead to those class labels attributes.

- Classification tree analysis is when the predicted outcome is the class to which the data belongs. In our proposed method classifies the various applications which are running on the virtual machine. Huge application and its APPLICATION FORUM to be identified.
- Regression tree analysis is when the predicted outcome can be considered as a user application ratio as a real number (e.g. the price of a house, or a patient's length of stay in a hospital). Regretting the virtual machine monitor elements in to a user application wall. USER SERVICE TYPE and LOCATION to be predicted from these approaches.

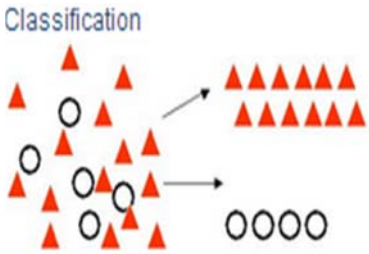


Fig: 1. (b) CLASSIFICATION TREE

Fig: 1. (c) REGRESSION TREE

3) SECURITY ASSUMPTION FACTORS

During the application deployment time as an auditor view we must focus the following objectives:

- Guests are untrusted
- Root must be trusted by hypervisor; parent must be trusted by children.
- Code will run in all available processor modes, rings, and segments
- Hyper call interface will be well documented and widely available to attackers.
- All hyper calls can be attempted by guests
- Can detect you are running on a hypervisor
- We'll even give you the version
- The internal design of the hypervisor will be well understood

AN EXAMPLE FOR CART

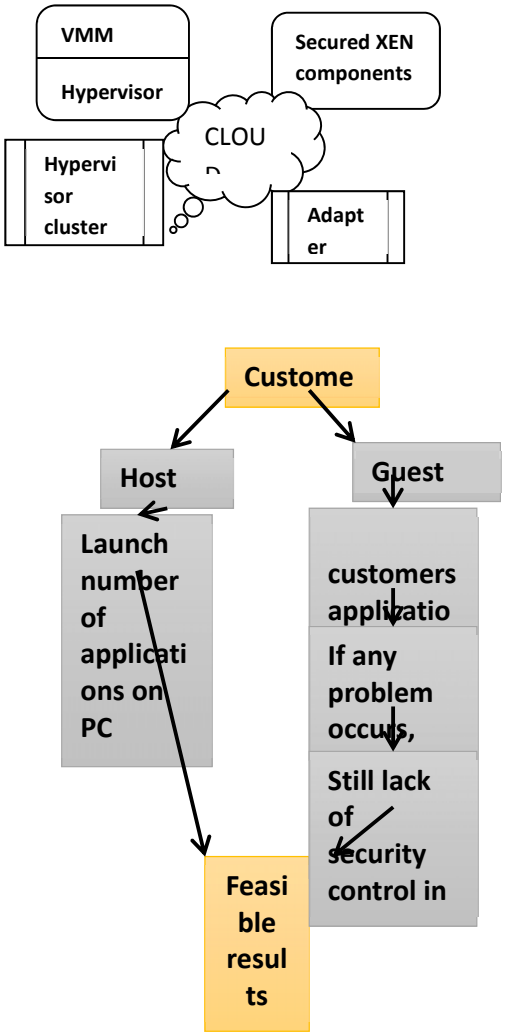


FIG: 1. (d) IMPLEMENTATION OF HYPERVISOR SECURITY PROBLEM

4) TRAINED HYPER-V MODEL

Aspect of this approach is, training the 2 layers in Hyper-V model based on the security factors partitioning, it also implements isolation of virtual machines in cloud environment. A partition is a logical unit of isolation, supported by the hypervisor, in

which each guest operating system executes. In VMware Vcloud Blog offers various utility packages for both private and public clouds. A hypervisor instance has to have at least one *parent partition*, running a supported version of Windows Server (2008, 2008 R2, or 2012). The virtualization stack runs in the parent partition and has direct access to the hardware devices. The parent partition then creates the *child partitions* which host the guest OSs. A parent partition creates child partitions using the *hyper call* API, which is the application programming interface exposed by Hyper-V. So, child partitions of thin ware and app ware

Fig: 1.(e) AN ILLUSTRATION OF VIRTUALIZATION SECURITY

- ❖ Hypervisor

It is majorly having two components:

- ❖ Virtualization Stack
- ❖ Virtual Devices

- It also requires hardware assisted virtualization
  - ➢ AMD AMD-V
  - ➢ Intel VT

Hypervisor survey is analysed for the various networks and cloud vendors. Cloud users will make use of this access in the cloud environment to run virtual machines and utilize the powerful server hardware. In order to allow users to use these virtual machines some type of virtual machine manager is needed. For this project, the XEN Hypervisor was chosen to fulfil this need. The hypervisor was installed on two servers located in the laboratory and allows users to remotely log in and create their desired machines.

- Trusted hypervisor components
  - ➢ Hyper guard – Phoenix Technologies – A hypervisor integrity scanner in SMM.
  - ➢ Deep watch – Intel project Virtualization root kit scanner
- Domain 0 Hardening component– Various security solutions to white-list and harden Domain 0.

5) IMPLEMENTATION ASPECTS

As a user focal point various factors have been considered. Main objective of the VMware is, allowing number applications to run in a single device. I had done some simulation type of results between the user applications with the hardware level applications. The results are given below and I have implemented the various stimulated results with the adapter tools such as:

- ❖ APP ware
- ❖ Thin ware
- ❖ VM ware
- ❖ VMWARE VCLOUD BLOG
- ❖ HYPERV
- ❖ VMWARE VCLOUD CONNECTOR

Service Type origin	Application type	Regretted values	Efficiency
Hypervisor controlling note	SAAS	ICV = 8.3	76.3%

Hypervisor Adapter kit	NAAS	ICV= 4.92	85.1%
Hypervisor APPWARE tool	PAAS	ICV=3.1	65.32%
Hypervisor SKEW tool	IAAS	ICV=5.83	78.31%

5.1) SIMULATED RESULTS & DISCUSSIONS

A user perspective, secured task is a major one. In this concept we are trying to prove the hypervisor problem and its recommended solutions. I had a simulation results while I am migrating the user application with virtual machine on cloud server. I was found some results for trained app ware and thin ware layers model that is follows:

User's IP address location	Mode of Application	Duration	Performance of task status
192.168.10.89	Exhibits organization profile	Deployment is done with 0.983 ms	Completed
192.168.26.94	Checking status for on-line education and services	Deployment is prohibited due to unsatisfied credentials	Migrated
192.156.23.87	User availability resources	Deployment is done with 23.56 ns	verified
192.162.45.71	Invalid attributes finding from users	Computed with in 8.3 s	demonstrated

Mathematical foundations are tested and verified with various user attributes. Efficient computation user level application hosting is:

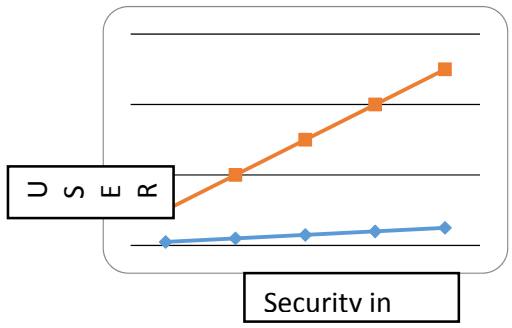
$\sum_{n=i-1}$ (Usr [x, y, zn] apps + VMM (threshold/0.3 *100)

Computation results= 93.47%

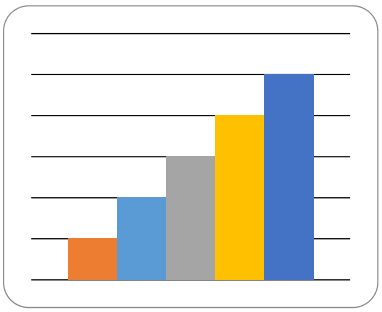
Eff = migrate from (65-97%) / attributes satisfied by hypervisor controller.

$\mu_{i=n}$ (credentials*0.83 – 34*100) / total applications which is deployed on virtual machine.

6) EXPERIMENTAL RESULTS



-



7) CONCLUSION

From this implementation of experimental results, the problem which is happening in

hypervisor i.e., majorly on security issues. So, we are providing various solutions like HYPERV, and the main feasible component is thin ware and APP WARE, SKE WARE. One of the main cost-saving, hardware-reducing, and energy-saving techniques used by cloud Providers are virtualization, With OS virtualization each VM can use a different operating system (OS), and each OS is isolated from the others. Use VMs to enabling different services to run in separate VMs

On the same physical machine. As an end user's able to rectify the security issues for numerous applications which are running on virtual machine with help of the mew mechanism is, NetWare in the future.

8) FUTURE DIRECTION

Cloud is a one forum which provides tremendous amount of advantages to its clients. But, customer feedback is an important one to evaluate the service. Still, the security issue is troubling the cloud users. We can able to direct the security focus in to the VM Theft and VM landscaping because, people are trying to hack the virtual machine. So in the future we need to bring the solution for VM attack and VM Theft.

9) REFERENCES

1. Author: chiwande V.N, Tayal A.R paper entitled as, "An Approach to Balance the Load with Security for Distributed File System in Cloud" – ICESC 2014.

2. Author: Shen Chen, Wenyu dong hang Li, peng Zhang, junwei cao paper entitled as, "Collaborative network security in multi-tenant data center in cloud computing" IEEE transaction volume-17, number 1, February 2014.

3. Author: Mendes. L.D.P, Rodrigues, Lloret.J, Sendra.S Paper entitled as, "Cross – layer dynamic admission control for cloud-based multimedia senor networks" IEEE transactions , 2014.

4. Author: Paper entitled as, "A Policy-Based Security Framework for Storage and Computation on Enterprise Data in the Cloud" IEEE transactions volume -4 march 2014.

5. Author: vijeng. L, Paper entitled as, "Security in the cloud based systems: Structure and breaches "Internet Technology and Secured Transactions (ICITST)-2013