Securing Virtual Images in Cloud Environment

Mr. Shiv Kumar Tiwari[1]*, Dr. Subhrendu G. Neogi[2] , Dr. Ashish Mishra[3]

[1]* Department of Computer Science Engineering, Amity School of Engineering and Technology, Amity University Gwalior Madhya Pradesh , India,sshiv.tiwari22@gmail.com

[2] Department of Computer Science Engineering, Amity School of Engineering and Technology, Amity University Gwalior Madhya Pradesh , India, sgneogi@gwa.amity.edu

[3] Department of Computer Science Engineering , Gyan Ganga Institute of Technology & Science , Jabalpur Madhya Pradesh ,India, ashish.mish2009@gmail.com

Article Info

Page Number: 7871 - 7882

Publication Issue:

Vol 71 No. 4 (2022)

Article History

Article Received*: 25 March 2022*

Revised*: 30 April 2022*

Accepted*: 15 June 2022*

Publication*: 19 August 2022*

Abstract

The new technology can offer on demand resources remotely with the help of new emerging expertise called cloud computing. Cloud computing helps users to work in an environment where physical infrastructure is not required at user end. There are many protocols which helps to access the resources provided by the cloud computing. Cloud computing is Internet based technology, which is charged on the basis of usage, demand and is offered to users of resources and services on them. The exact location where the user is to be configured is hidden from all cloud servers.. In the proposed work, user-generated secure key is used for authentication and at the time of virtual machine (VM) switching. Every time when a user requests for a new service from another VM, it has to authenticate. To authenticate genuine user, a secure pass key is used every time, it ensures security and authentication between system and user.

Keywords - Cloud Computing, Cloud Security, Virtual Machine (VM), VM Switching.

I. INTRODUCTION

The cloud computing is a key technology such as hardware, software and application development as all the computing resources are provided to the customers through internet platform. Explicit mediocrity refers to different IT environments dedicated to providing measurable and resources of measurable IT. The expression originated as short metaphor for Internet, a set of IT resources to provide remote access to the network's decentralization of the network. Various features typically represented the Internet in a web-based architecture before becoming a formal IT industry segment

for the main cloud computing and cloud documentation icons. The construction of security privacy is driven by the 3 significant characteristics of block construction, availability and integrity, which is a very secure system. Protects data, hardware aspects and software resources. Check data integrity is compromised. This is anytime and anyplace for the users to ensure availability and it can also use resources and services also guaranteed to process the data available [2]. The mission is achieved by business continuity planning (birth control pills), which uses redundancy to ensure the availability of critical systems. Confidentiality is defined as given access only to persons those are authorized. An unauthorized access may use data, loss of privacy. This can be done in two ways, electronically or by anyone. So the loss through communal problems, the so-called loss of physical privacy. Damage occurs when the client and server their communication is not encrypted, this is known as loss of electronic privacy. Security and privacy are key to the achievement of cloud computing as well as the most challenging issues. Leading data for efficient ownership history data records and log forensics. In cloud systems, digital fingerprints [4] sent for the confidentiality of storage of sensitive documents from the original scheme. Action is taken to provide the user digital fingerprint images with a highly secure cloud computing. Hash values or messages only digest a small amount of text or a text string. It is produced by a well-defined formula that the same hash value is too low for two-wire outputs. Use the hash value that is used to make sure that a secure system does not produce data back. The message generates a hash value of the encrypts and sends the message. The receiver then decrypts the message and either hash and generates another message decrypted hash. If two hashes are the same, this indicates that there is no change in the data during transmission. The 128 bit hash will be a digest text as stated in the message.

1.1 Cloud Characteristics

Effectively scalable IT environments and remotely measured IT resources require a different set of measured supply possibilities. Effective cloud IT environments require this feature to be present to a large extent.

Here are 6 of the most common special features for cloud environments:

- On-demand access
- Universal Access
- Multi tenancy (outsourcing pooling)
- Elasticity (and scalability)
- using measured
- Flexibility

Cloud Computing Architecture consist of two layers: Front end and Back end. Client works on front end which compromises of applications and the interface to access cloud. Back end handles all resources, security, virtual environment and traffic management. Cloud computing manages the workload by providing h/w and s/w services in virtual way. It covers three strong areas required by the users.

(1) Storage

(2) Computing

(3) Networking.

Components of cloud computing

1) Management software

2) Deployment software

3) Storage of cloud

4) Server of cloud

5) Route of connectivity

6) Hypervisor

1) Management software: All time access from anywhere facility is given to the user by maintaining and configuring the infrastructure.

2) Deployment software: Its all deal with installation and configuration of the software on the cloud.

3) Storage of cloud: this says about cloud storage server on web.

4) Server of cloud: to avoid the problem of physical server cloud server introduced virtually to run the programs independently.

5) Route of connectivity: virtual route to connect cloud services over the internet..

6) Hypervisor: this gives user an operating virtual platform. It's a firmware.

Cloud providers can measure consumer cloud hunting individually and collectively evaluated the value of the cloud platform given these characteristics. Cloud-based services and IT resources will individually distinguish and display different attributes, then generally they are supported and utilized so far resulting in a higher value proposition.

1.2 Cloud Delivery Models

The cloud distribution model is the resources offered by the typical combination of pre-packaged cloud IT providers. Three public cloud distribution models has been broadly established and become official:

- Infrastructure-as-a-Service (IaaS)- IaaS as per name provides whole infrastructure to the cloud, flexibility, portability.

- IP address
- Load balancing
- VLAN
- Virtual Storage

Platform-as-a-Service (PaaS)- PaaS as per name provides platform to the cloud. It is middle ware which handles operating system, storage, Runtime applications.

- Google Drive
- AWS
- Window Azure
- Apache Stratos

Software-as-a-Service (SaaS)- This helps non technical companies to get connect with other two Architecture. On which architecture we have to work is dependent on few parameters: like timeline, team and plan.

- Google APPS
- Dropbox
- Mail
- Paying bills

1.3 Cloud Deployment Models

The cloud deployment model is primarily proprietary of the cloud environment, which is a special type of size and range. There are 4 types of cloud deployment models:

- Community Clouds
- Public Clouds
- Hybrid Clouds
- Private Clouds

1.4 RISKS AND CHALLENGES

Cloud in the cloud customers' reward many of the most important challenges for investigating the use and computing of public cloud IT resources.

This segment covers the subsequent topics:

• Increased security flaws

• Low operating governance control

• Limits between portability of cloud providers

• Multi-sectored regulatory and legal issues

1.5 Increased Security Vulnerabilities

Responsibility for carrying business data into that cloud protection cloud instrument with the cloud provider. Remote access to IT resources needs to expand the boundaries of cloud consumer trust to combine external cloud. It may be different to introduce a security structure difficult to build confidence boundary propagation without vulnerabilities, as long as it supports the same security framework or persistent cloud consumer and cloud provider - which is possible with public cloud Is not.

Another result of trust is overlapping limitations of accessing particular consumer cloud data by the cloud provider. As far as data is protected, this cloud is limited to the consumer so far and is implemented by both cloud provider security controls and policies. In addition, because it is generally divided on cloud-based IT resources, the limits of different cloud consumer religions can overlap. Limitations of IT resources can provide dangerous cloud consumer confidence and an increased risk of data (human and automated) and more opportunities to attack or transmit business data, theft damage. This rate is such a scenario, showing that two organizations with the use of cloud services have the same requirement to expand the boundaries of trust associated with the cloud, resulting in the discontinuation of the power of trust.

1.6 DATA CENTER TECHNOLOGY

Geographic spread has occurred rather than one another, enabling IT resources to be classified in proximity to IT resources with higher efficiency sharing enabled use, and better utilization for shared IT personnel. This one advantage naturally makes it limited to the data centre concept. Modern data centres are used for centralized IT infrastructure as well as resources used by specific IT servers, databases, networks and telecommunications equipment and software systems.

Data centres are typically comprised of the following technologies and components:

- Automation
- Standardization and Modularity
- Virtualization

- Security-Aware Design, Operation, and Management
- High Availability
- Remote Operation and Management
- Storage Hardware
- Computing Hardware
- Network Hardware

1.7 VIRTUALIZATION TECHNOLOGY

Virtualization is the technique of changing a physical IT resource into an IT resource which is virtual. Most types of IT resources can be virtualized, including:

Server - Abstract is enabled for physical servers in virtual servers.

Storage - Physical storage space devices can be summarized into virtual storage devices or virtual disks.

Network - can be expressed in a physical router and fabric logical network switches, like VLANs.

Power - Physical power supply units are usually referred to as virtual UPS.

The first step in creating a new virtual server with virtualization software is followed by the physical IT resources an allocated operating system allocates. The virtual server has its own hotel operating system, which is independent of the operating system in which they were created.

Guest OS and applications of virtualization software process running on a virtual server, are not aware of, which means that the virtual settings of the resources and they run on a different physical server. An important feature of virtualization is because of the consistency of performance that allows you to run programs on a physical system to a virtual system. Each operating system software products and applications require the use of a common seamless virtual environment, configured, or that do not need to be optimized to run patches.

Virtualization software created host or host is a physical event called physical server, can be achieved with hardware virtualization software. Virtualization software also includes system management functions, and services related to a particular virtual machine, typically not a standard operating system. Software that is sometimes known as Virtual Machine Monitor (VMM) or Virtual Machine Manager but commonly known as Hypervisor**.**

1.7.1 Hardware Independence

The operating system and application software configuration produced several software-hardware dependencies to install the IT hardware platform. In non-virtual environments, you need to modify

these IT resources when the operating system needs to be re-aligned with models configured for specific hardware needs.

Virtualization is a changing process that acts as IT hardware and software that is translated into copying by default. Through H/W independence, virtual servers can simply be shifted to a different virtualization host machine, automatically to resolving many hardware-software incompatibility issues. As a result, little manipulation cloning and replicating virtual IT resources and easy physical hardware. A part of this book, an architectural model, is also provided some examples.

1.7.2 Server Consolidation

Coordination of tasks will be made available virtualization software that allows the same virtualization host to be performed in multiple virtual servers simultaneously. Virtualization technology allows you to share a physical server to a different physical server. This process is called consolidation server and is provided using resources and IT is used to improve optimization of hardware load balancing. Flexibility, resulting in the same host if you can run a variety of guest operating systems on different virtual servers. This is such a feature as public cloud demand access, resource pooling, and elasticity, efficiency on computing facilities, and flexibility, support.

1.7.3 Operating System-Based Virtualization

Operating system virtualization software is currently based OS, which is a pre-established virtualization, called host operating system. For example, it has been decided to install a special version of Windows on the user workstation that he wanted to create a virtual machine. Such applications as other programs on the operating system software and this set of virtualization hosts use this application to generate one or more virtual machines and run. A virtual machine must be generated to reach the user directly using virtualization software. Because the host operating system can provide the hardware with the necessary support, the system compatibility point of hardware virtualization can improve operating, even lost is the rider hardware virtualization software.

Hardware virtualization enables hardware independence enabling the use of IT resources more flexible. For example, in situations where software is available to a physical computer on the host operating system, up to five network cards are needed to control. Virtualization software can provide up to five network adapters for a virtual machine, even virtual operating systems typically five network adapters with physical disabilities. Hardware virtualization to software and IT resources that are virtual IT resources to different operating systems that is compatible with the

needs of this unique software for operation. Because the host operating system is complete in the operating system itself, so management is operating system-based services and government organizations can use a virtualization host to manage assets as a tool.

1.7.4 Virtualization Management Many administrative tasks can easily be performed using their physical counterparts as a counterweight to virtual servers. Modern virtualization software provides many advanced management functions that can automate government and virtualization tasks that can reduce the overall operational burden on IT resources. Virtualization of IT management resources often relies on virtualization infrastructure management (VIM) devices that must support controlling IT resources to manage and run virtual mass-run centralized management modules, which are primarily known computers. Vim is covered by a system of public resource management systems.

1.7.5 Web Applications

A distributed application that relies on web browsers for the presentation of user interfaces using web-based technologies (and usually) are usually treated in a web application. All types of applications can be found due to high penetration in cloud-based environments. Abstract Web Common Architecture for web applications is based on the three-tier award model. The first category is called the presentation layer, which represents the user interface. One is a mid-level application layer that implements the application logic, while the third layer involved in the data rate is a permanent repository.

Chapter 2

II. SURVEY OF LITERATURE

Author in paper [1] proposed method to monitor user activity and to find out if a proposal based on a Virtual Machine Introspection (VMI) Malicious Security Framework. They said that to discuss the main advantages of the proposed framework, it was decided to implement other methods of VMI method based on material knowledge. They are capable of analyzing the proposed design of virtual machines hosted on the cloud. A multi-threaded server component can be extended in real time. Experimental results suggest that the structure IaaS clouds perform well with a set of measures and parameters suitable for the cloud environment. They stated that the monitoring and their characteristics of virtual machine process call classification process systems are described in our modified model vector space. The proposed framework, which is specifically designed to host multiple VMs on multiple physical machines to run multiple processes.

In the paper [2], the authors discussed the performance of resource allocation algorithms that use CPU best time and memory. They showed how to handle live migration of virtual machines in cloud computing across the cloud. They suggested a possible resource migration algorithm for optimal use of unused memory VMs. In the memory process occupied setting off, VM and persistent memory probably occupied for VM memory and total memory demand. Our proposed algorithm has not been published as part of the efficient use of memory, and we VM total stack flow architecture of cloud storage memory measurement work.

The authors [3], who have made progress, propose the identity modified bus technology and modify the content of VM memory pages and only the dirty content. The proposed technique intensive workload virtualization environment configured on QEMU-KVM revealed by VM. Results show that in a copy of the former VM immigration plan to readintensive workloads, we provide technology that is 69.4%, 73.5% possible, and reduces downtime for network traffic by 74.21%. Similarly, for write-intensive workloads, downtime, migration time and network traffic decreased by 47.23, 49.16 and 51.37%. Thus, the proposed technique has increased effective performance VM migration planning.

Paper [4], authors proposed a Trusted Computing Security Framework Security for VM's Life Cycle. The use of the proposed framework they achieved the integrity and security of VMs a reliable technology life cycle. In particular, the concept of life cycle VM presents the breakdown of the various operating conditions of VM. Then, to develop a computational-based security framework that is reliable, trusted relationship platforms can be the way to extend VM modules and protect the security of trusted VM life cycles and reliability. Theoretical analysis suggests that a comprehensive security framework for TV can be supplied by M is offered in all states. In addition, it is possible to use the results of events to offer a higher level of security structures and some sophisticated schemes.

The paper [5] authors have proposed a security framework to protect the virtualization layer in the cloud environment image of a virtual machine. In order to maintain the image of a virtual machine, as it can affect is necessary to protect cloud computing. Multi tenancy is also an introduction to the problem and issue of the VMs virtualization layer, affecting VMM and OS. The initial state of the infected VM can affect the security of the VM images. Therefore, to protect the VM images, a structure are projected which is able to secure the stored VM image in the repository In the paper [6], the authors have attempted to defeat the restraints of existing h/w support. In particular, authors

proposed safe and efficient protocol designed to take privacy, integrity, access control standard and non-abandonment basic security services, the destination domain includes a domain account cloud virtual machine resource cloud. The proposed protocol enabled local authentication and authorization of the client as possible. Authenticated digital domain signed through ticket exchange using FIPS-196 on sources in both destination domain authority servers. Generate a symmetric session key at both ends of the encrypted AES during the transition of data to the VM using ECDH and access and data integrity using SHA-256. In addition, not only the domain power protocol makes the message exchange order less than the difference in achieving mutual authentication domain, but efficient.

The paper [7] Proposed, combines intrusion detection and technology with a run on virtual systems to provide reliable technology for intrusive policy-based distributed applications provide integrated security control integrated security structure. A physical server security structure of their virtual interaction between applications and virtual machines on security access control security policy. Intrusion detection is an efficient way to explore dynamic attack and working with them and to provide a reliable verification technology. They use for evaluation Decision Evaluation Engine (DEE), Entity Validation (EV), Information Capture and Logging (ICL), Taint Analysis (TA). They showed how to use integrated security structure for virtual machine life cycle including dynamic allocation of resources for various physical servers.

III. PROPOSED DESIGN

Cloud computing helps users to work in an environment where physical infrastructure is not required at user end. There are many protocols which helps to access the resources provided by the cloud computing. Cloud computing is Internet based technology, which is charged on the basis of usage, demand and is offered to users of resources and services on them. The exact location where the user is to be configured is hidden from all cloud servers. Research is to improve performance while reducing costs. In the proposed work, user-generated secure key is used for authentication and at the time of virtual machine (VM) switching. Every time when a user requests for a new service from another VM, it has to authenticate. To authenticate genuine user, a secure pass key is used every time, it ensures security and authentication between system and user. To minimize idle time of virtual machine, a session timer is used in each VM for every user.

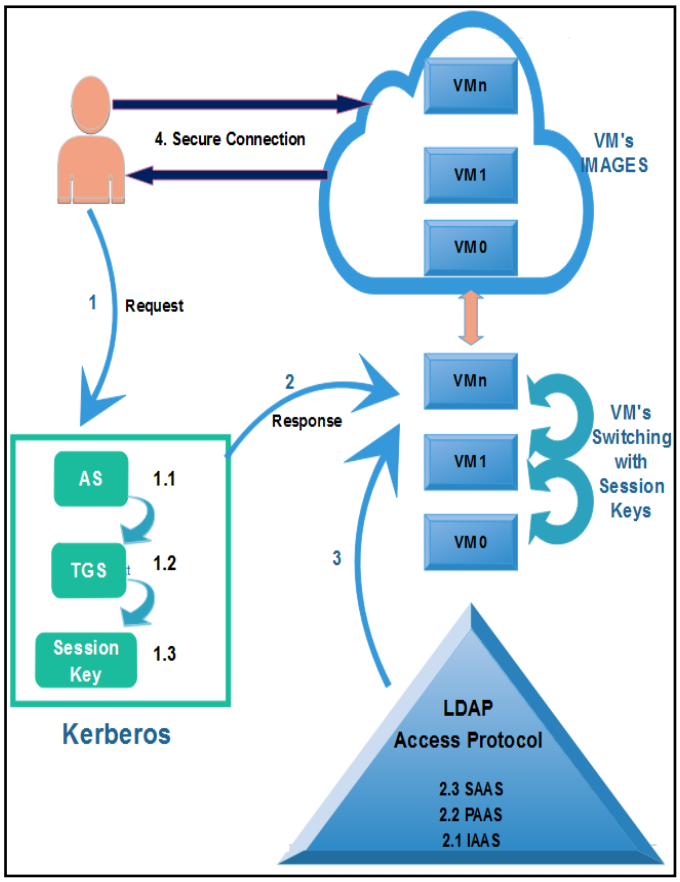

Figure : Proposed Architecture for Secure Virtual Image Switching

IV. EXPECTED OUTCOME

- The Quality of the system proposed should give the better results as compared to existing methods.
- More Secure virtual image as compared to existing systems.
- It provides high level security features.

REFERENCES

[1]. Bhavesh Borisaniya and Dhiren Patel, "Towards virtual machine introspection based security framework for cloud", Sådhanå (2019), Indian Academy of Sciences.

[2]. Souvik Pal, Raghvendra Kumar, Le Hoang Son, "Novel probabilistic resource migration algorithm for cross‑cloud live migration of virtual machines in public cloud" © Springer 2019.

[3]. Aditya Bhardwaj and C. Rama Krishna, "Improving the Performance of Pre-copy Virtual Machine Migration Technique", Proceedings of 2nd International Conference on Communication, Computing and Networking, © Springer Nature Singapore Pte Ltd. 2019.

[4]. Xin Jin, Qixu Wang,Xiang Li, Xingshu Chen, and Wei Wang, "Cloud Virtual Machine Lifecycle Security Framework Based on Trusted Computing", Tsinghua Science and Technology, Volume 24, Number 5, © IEEE 2019.

[5]. Raid Hussein, Ahmed Alenezi, Gary Wills, Robert John Walters,"A Framework to Secure the Virtual Machine Image in Cloud Computing", International Conference on Smart Cloud, 2016 IEEE.

[6]. Tayyaba Zeb, Abdul Ghafoor, Awais Shibli, and Muhammad Yousaf, "A Secure Architecture for Inter-cloud Virtual Machine Migration", © Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015.

[7]. Vijay Varadharajan, Udaya Tupakula, Member, "On the Design and Implementation of an Integrated Security Architecture for Cloud with Improved

Resilience", Transactions on Cloud Computing©IEEE 2015.

[8]. Mell, Peter and Grance, Tim, "The NIST Definition of Cloud Computing", Version15,October7,2009,http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[9]. The NIST Definition of Cloud Computing (SP 800-145)Oct25,2011 is available at http://csrc.nist.gov/publications/PubsSPs.html#800-145.

[10].https://docs.openstack.org/security-guide/introduction/introduction-to openstack.html.

[11] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez,

"An analysis of security issues for cloud computing," J. Internet Serv.Appl., vol. 4, no. 5, pp. 1–13, 2013.

[12] F. Sabahi, "Virtualization-level security in cloud computing," in 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 250–254.

[13] S. Carlin, "Cloud Computing Security," Artif. Intell., vol. 3, no. March ,pp. 14–16, 2011.

[14] J. Kabbedijk, C.-P. Bezemer, S. Jansen, and A. Zaidman, "Defining multi-tenancy: A systematic mapping study on the academic and the industrial perspective," J. Syst. Software, vol. 100, pp. 139–148, 2015.

[15]TiwariS.K.,Rajput.,D.S.,Sharma,S.,Neogi,S.G.,and Mishra, **"**Cloud Virtual Image Security For Medical Data Processing" in A Mathematical Modelling and Soft Computing in Epidemiology**,**Taylor & Francis Group, chapter 17**,** 2020. https://doi.org/10.1201/9781003038399

[16] Tiwari, S.K., Neogi S. G., Shakya H.K., Mishra A.,Devaraju T., (2022). Design and Implementation of a Virtualization Security Technique for Cloud Computing. *Computer Integrated Manufacturing Systems*, *28*(12), 114–123.