Virtualization in Cloud Computing Environments

Aruna Malik, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - aruna.malik@galgotiasuniversity.edu.in

Abstract: ***Virtualization has become a widely and attractive employed technology in cloud computing environments. Sharing of a single physical machine between multiple isolated virtual machines leading to a more optimized hardware usage, as well as make the migration and management of a virtual system more efficiently than its physical counterpart. Virtualization is a fundamental technology in a cloud environment. However, the presence of an additional abstraction layer among software and hardware causes new security issues. Security issues related to virtualization technology have become a significant concern for organizations due to arising some new security challenges. The report discusses the major challenges and risks associated with virtualization of cloud environments. It also concentrates on certain specific cyber challenges and attacks that impact cloud protection. The survey analyzed cloud stakeholders ' views on virtualization weaknesses, risks and solutions to resolve these vulnerabilities.***

KEYWORDS: ***Cloud Computing, Virtualization, Security, Challenge, Risk management, Data protection.***

INTRODUCTION

The architecture of a cloud-based infrastructure is based on virtualization technologies. It enables many operating systems identified as a virtual machine (VM) to co-locate on the same physical server and use the hierarchical resource resources without intervening [1]. In many cases of the same program, virtualization helps to run on one or more cloud services. The virtualization layer includes the scalability dynamically, so multiple users will concurrently execute their code [2]. It allows the user to operate his / her own applications on a single VM and not to access the data from other devices. Vol 11, No 3, June 2019 96 Virtualization technology is useful for anyone using a computer, commercial companies and governmental agencies as well as IT practitioners. International Computer Journal & Information Technology (IJCSIT) Vol 11,

We offer organizations and people the chance to use their equipment and develop it by increasing the number and kinds of tasks a single computer is capable of carrying out. In a virtualization environment, the sharing of resources and isolation are two significant benefits [3]. The separation, VM isolates own data from other VM, is also an advantage that the virtual world may provide. The malfunction of one VM does not affect the performance or the execution in the same set of other VMs. The ability of users to use other VMs or the capacity of other VMs to have access to resources on the same network, if the VM malfunction, will not be impaired [4]. In fact, isolation ensures that one Server system cannot see others operating on another Machine. It can be inferred that the different VMs will share the physical machine's resources without intervention. These functions provide for the stable and continuous running of multiple operating systems and applications on a single physical unit [5].

In terms of its features, software, surveillance and protection procedures, stability is a hot issue in virtualization. The privacy, anonymity and quality of cloud services and resources was compromised by multiple bugs, hazards and threats on the vision layer. This research aims at defining and recognizing the main challenges and security issues in cloud computing. It also provides guidance for technology enhancement and virtualization of risk mitigation in order to implement safe cloud computing [6]. The majority of the document is written like this. Security problems and threats of virtualization are discussed in the next segment. Section III identifies major attacks that could challenge applications for virtualization. Section IV addresses survey results and analyzes. Ultimately, Section V provides practical guidance and suggestions for avoiding or alleviating potential threats to virtualization.

Fig 1. Cloud Computing

Security Challenges and Risks

This section investigates set of common vulnerabilities and risks of virtualization in cloud computing environments. User awareness: In terms of information protection, cloud services applications are the weakest point since Cloud service companies do not test their consumers ' settings. Suspicious user accounts will require attackers without being identified to do any wrong work. In fact, there are intrusion methods used by an intruder to manipulate a target into accessing a malicious website to gain access to the user's computer. This allows user behavior to be tracked and the same details as the customer does and user passwords to authenticate the cloud services itself. Knowledge of vulnerability is a security issue which is often neglected. The misuse of transparent cloud services by consumers also helps an intruder to enter the network, allowing users to know of various possible vulnerabilities and how to keep them from knowing and taking over their duty [7].

Insecure APIs

A cloud computing network provides customers with hardware, applications and application tools and encourages them to use their interfaces. The programs have been written to develop their interfaces. According to APIs will impact the quality and protection of cloud services by presenting many security issues, such as inadequate authorisations, low credentials and clear-text communication.

Lack of security policies:

In order that its properties can be secured from possible risks and how these circumstances are dealt with, the organisation determines security policies. The company The Cloud service provider's security policies may not be appropriate or inconsistent with the organization's safety requirements [8]. Failure to implement security policies will lead to some vulnerabilities in the vulnerable VM setting.

Weak authentication and session management:

Authentication is the method for deciding whether or who is proclaimed. Authentication code defends the device from unauthorized actors masking the read, erase and change data as authorized users, developers or operators. The security function for both end users and system components is valid in a virtual environment. Authentication and session management features improperly planned or applied can have an effect on access and control policy [9]. Moreover, it enables attackers to compromise keys, session tokens, or passwords and to exploit flaws of other implementation to assume other identities of users.

Incorrect VM isolation

The hypervisor maintains separation between the different VMs. The separation of VMs prohibits the simulated drives, applications, or memories of other users on the same host. In fact, VM separation reduces the attack's reach. It makes access resources, and sensitive data on the physical machine complicated.

Insecure VM migration/mobility

One of the many benefits of Virtualization is a live migration strategy, which enables the code to be transferred transparently from one host to another without stopping the VM. The program will be conducted without lack of development following migration. The consumer does not realize that his Machine has shifted. The VM can be transferred to the destination host by transferring the configuration of the VM with the complete system condition such as memory, CPU status and sometimes disk. The intruder may, however, actively intercept or snoop or alter confidential information during the migration process [10].

VIRTUALIZATION THREATS AND ATTACKS

Cross-Vm Attack

Cross-VM attack occurs when the hypervisor level isolation is ignored by a malicious virtual machine to attack co-located VMs. According to X-VM attacks, the use of guest and hypervisor weaknesses to access the secret data through side channel attacks varies from other VMs to managed attacks. Many VMs are positioned on one server to increase the resource utilization, which could trigger cross VM side channel assault. This co-resident positioning. The underlying possibility for a cross-VM side channel assault is through a co-location intrusion and inadequate separation procedures; a malicious VM commits side channel attacks. The hypervisor will split a VM while operation, take a current disk snapshot, memory, Processor statements and recover a snapshot without VM knowledge in future.

The VM maintenance and resistance trait was used, however the attacker is able to launch VM rollback attack [11]. The intruder can use VM's previous snapshots, execute them without the user's knowledge, then take the VM execution history and run the same snapshot or the same one again. Since the past of execution of the VM is missing, certain security mechanical mechanisms or some protection mechanisms may be prevented by the attacker.

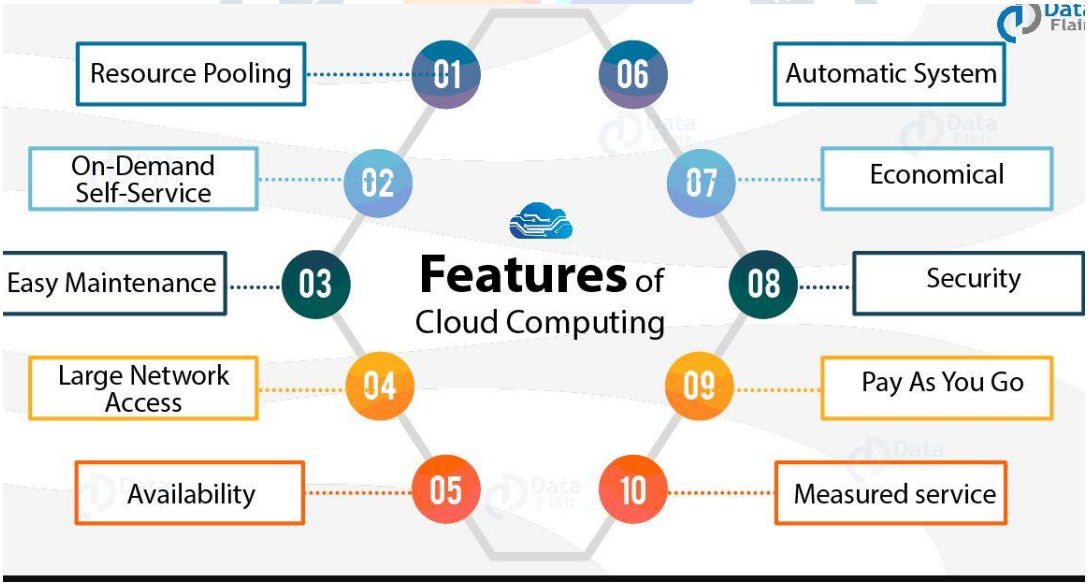

Fig 2. Resource of cloud computing

Data Loss and Data Leakage

Data leakage generally occurs when sensitive information is distorted as audited, handled, analyzed, or distributed. In the event of a lack of encryption or of an unintended deletion a loss of data happens when saving data is destroyed [12].

Survey Results and Analysis

It study seeks to collect feedback on weaknesses and risks to cloud storage from faculty members, graduate students and IT personnel and identify effective security strategies used to mitigate the security

risk of virtualization. 127 individuals engaged in this study. Based on these research questions, the sample is prepared.

CONCLUSION

Cloud virtualization provides an easy way to set up new virtual servers, so you don't have to manage many servers. It's important to keep track of where everything is and how physical resources are being used for virtual resources, so buy a solution that includes easy-to-use tools to help you measure and monitor usage. Virtualization doesn't solve every problem for everyone. But in most cases, virtualization is becoming more and more popular as the benefits of efficiency, performance, security and cost outweigh all issues.

REFERENCES

[1] Aaqib Rashid, Amit Kumar "Cloud Computing Characteristics and Services: A Brief Review", International Journal of Computer Sciences and Engineering Vol.7(2), Feb 2019, E-ISSN: 2347-2693

[2] Michael Kretzschmar, S Hanigk, "Security management interoperability challenges for collaborative clouds", Systems and Virtualization Management (SVM), 2010, Proceedings of the 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and the Cloud, pp. 43-49, October 25-29, 2010. ISBN:978-1-4244-9181-0,DOI: 10.1109/SVM.2010.5674744.

[3] B. Loganayagi, S. Sujatha, ―Creating virtual platform for cloud computing‖, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2010), 28-29 Dec. 2010, pp.1-4.

[4] Dawei Sun, Guiran Chang, Qiang Guo, Chuan Wang, Xingwei Wang., ―A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques‖, First International Conference on Pervasive Computing, Signal Processing and Applications (PCSPA); 2010, pp.305-310.

[5] Karen Scarfone, Murugiah Souppaya, and Paul Hoffman, ―Guide to Security for Full Virtualization Technologies‖, Special Publication 800-125, National Institute of Standards and Technology (NIST), 2011.

[6] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, ―Xen and the art of virtualization‖, in: Proc. 19th ACM Symposium on Operating Systems Principles, SOSP 2003, Bolton Landing, USA, Oct. 2003.

[7] Joanna Rutkowska and Alexander Tereshkin, ―Bluepilling the Xen Hypervisor‖, Xen 0wning Trilogy part III, Black Hat USA, aug 2008.

[8] Samuel T. King, Peter M. Chen, Yi min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch, ―Subvirt: Implementing Malware with Virtual Machines‖, In IEEE Symposium on Security and Privacy, 2006.

[9] Z. Pan, Q. He, W. Jiang, Y. Chen, and Y. Dong, Nestcloud: Towards practical nested virtualization,‖ in Proc. Int Cloud and Service Computing (CSC) Conf, 2011, pp. 321–329.

[10] W. Dawoud, I. Takouna, and C. Meinel, Infrastructure as a service security: Challenges and solutions‖, in Proc. Informatics and Systems (INFOS), 2010 The 7th International Conference on, 2010, pp. 1 –8.

[11] Calheiros RN, Buyya R, De Rose CAF, ―Building an automated and self-configurable emulation testbed for grid applications‖, Software: Practice and Experience, April 2010; Vol. 40(5), pp. 405–429.

[12] Asma ben letaifa, Amed haji, Maha Jebalia, Sami Tabbane, ―State of the Art and Research Challenges of new services architecture technologies: Virtualization, SOA and Cloud Computing‖, International Journal of Grid and Distributed Computing 3(4), December 2010, 69-88.