Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 22 Issue 1, January 2020

In Cloud Computing, Towards a Trusted Launch Mechanism for Virtual Machines

Mr. Kuldeep Chauhan, Dr. Mamta Bansal

Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut

Email Id- kuldeep.chauhan@shobhituniversity.ac.in, mamta.bansal@shobhituniversity.ac.in

ABSTRACT: ***Although cloud computing allows us to dynamically provide servers with the flexibility to meet a broad variety of requirements, it also introduces a slew of new security concerns. One of the most pressing concerns for cloud computing is the security of virtual machines (VM). Existing VM security methods, such as Terra, toot, and TXT, however, are primarily concerned with the security of the VM operating environment. In clouds, there is no protective mechanism for virtual machines (VMs). We present a trusted launch solution for virtual machines (TLVM) in this article, which includes four systematic methods for safeguarding VMs in clouds: image encryption, measurement, attestation, and security-enhanced authentication. A proof-of-concept implementation of our method is also discussed. The results of our tests show that our technology can secure the whole launch process of a virtual machine. The measurement module will then take measurements on the virtual machine picture. The measurement outcome, including the measurement value and a signed report data from the host is transmitted to a remote attestation server for verification. The image's integrity the user will use the Usbkey to log into the VM. The virtual machine will connect to the host and get the migrated key.***

KEYWORDS: Attestation, Cloud, Measurement, Security, Virtual Machines (VM).

1. INTRODUCTION

Because it offers an expandable and powerful environment for increasing quantities of services and data, the new cloud-computing paradigm is quickly gaining traction as an alternative to conventional information technology. The security of existing cloud infrastructures, on the other hand, is a major issue that is likely to stymie cloud computing growth. Virtual machines are leased to customers for infrastructure as a service (IaaS) in cloud computing. The virtual machines hold certain sensitive user data. Users' interests will be jeopardized if data is spilled outside of virtual computers. As a result, in IaaS, how to protect the security of virtual machines is critical. However, current VM security methods such as Terra , TXT , and tboot are primarily concerned with the security of the VM operating environment, such [1] .

To secure virtual machines, TLVM employs four systematic mechanisms: image encryption, measurement, attestation, and trusted-enhanced authentication. The image encryption technique may prevent unauthorized users from launching a virtual machine. A VM's integrity may be protected via measurement and attestation methods. A user and a virtual machine may both be authenticated using the trusted-enhanced authentication method. As a result, the whole system can safeguard the entire VM launch process in cloud computing. The rest of this paper is laid out as follows. In .2, we outline our objectives and the TLVM architecture; we describe the architecture of our systematic method for VM security protection. The implementation of TLVM is discussed in [2].

1.1. Model of Trust and Attack

An administrator may copy VM images outside of a trusted domain in our trust and attack concept. Trusted nodes make up the trusted domain. Tboot, TXT, and dynamic measurement technologies, such as SICE and TEE may be used to create trusted nodes, which include hosts and VMM. In addition, attackers, even IaaS managers, may tamper with VM images. Furthermore, since a user cannot trust the VM's identity, the user is vulnerable to a VM phishing assault. In the present attack model, a VM instance is deemed trustworthy if and only if it meets the following criteria:

(1) The instance's VM image has not been tampered with.

(2) A trustworthy domain is used to start the VM instance.

(3) The VM's identity may be trusted.

Tboot, TXT, and dynamic measurement technologies, such as SICE and TEE, can ensure the second of the above requirements. The paper's main emphasis is not on these techniques. Instead, we'll look at the VM launch's trust problem [3].

1.2. General Information

The Trusted Computing Group has created and advocated a technology known as trusted computing. A computer will consistently act in anticipated ways with Trusted Computing, and these behaviors will be enforced by computer hardware and software, trustworthy chain based on trusted base is used to enforce such behaviors. To guarantee the confidence of a protected platform, five major key technologies may be used: endorsement key, secure input and output, memory protected execution, sealed storage, and remote attestation. TLVM is a security protection method for virtual machines on a cloud computing platform that is based on trusted computing technology and can ensure the confidentiality, integrity, and authentication of a user's VM.

In VMM, we add the image encryption, measuring, and attestation modules in TLVM. In addition, VMs include an authentication module based on Usbkey and a trusted platform module (TPM). These methods provide a methodical approach to starting a virtual machine in a safe manner. A cloud management center with a user management module, a VM management module, a key management and attestation server, a host with virtual machines, an Usbkey administrator, and users make up the system. Figure 1 discloses the Trusted [4].

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 22 Issue 1, January 2020

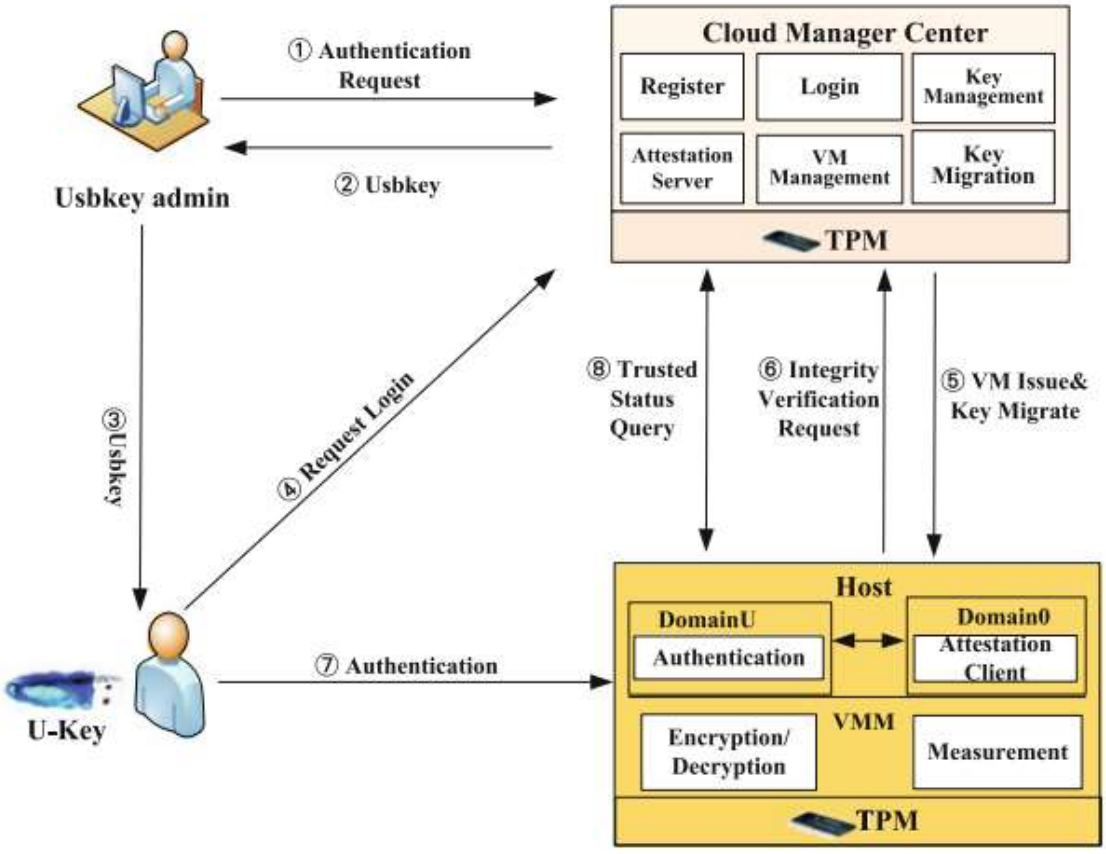

Figure 1: Illustrating a Trusted launch process of a VM.

2. DISCUSSION

A certificate, a private key, and a symmetric key are requested from the cloud management center server by a Usbkey administrator. A certificate, a private key, and a symmetric key are generated by the cloud management center and written to a Usbkey. Meanwhile, the storage key is encrypted using the symmetric key. Towards a Trusted Virtual Machine Launch Mechanism 93On the cloud management server, the root key (SRK) of the TPM will be stored. the key management center in the cloud The Usbkey is given to the user by the Us key administrator [5].

The user accesses the cloud administration center and submits an application for a virtual machine. Machine. For the user, the cloud management center builds a virtual computer. A host is used to execute the encrypted virtual machine image. Meanwhile, TPM key migration will transfer the symmetric key to the host. After that, the local TPM will safeguard you. The picture encryption in VMMThe picture will be decrypted using the migrated symmetric key by the decryption module. The measurement module will then take measurements on the virtual machine picture. The measurement outcome, including the measurement value and a signed report data from the host is transmitted to a remote attestation server for verification. the image's

integrity The user will use the Usbkey to log into the VM. The virtual machine will connect to the host and get the migrated key. Both the VM and the user will cooperate. Authenticate using the Usbkey's symmetric key and the migrated key. When the user logs onto the virtual machine. The attestation server will interact with the trust inquiry module in VM to get the VM's measured result. Then On the VM's desktop, the trusted status will be shown. Image encryption/decryption, measurement, attestation, and a security-enhanced method based on TPM are all included in TLVM.

The in-depth analysis the following is a description of their design. VM Image E A certificate, a private key, and a symmetric key are requested from the cloud management center server by a Usbkey administrator. A certificate, a private key, and a symmetric key are generated by the cloud management center and written to a Usbkey. Meanwhile, the storage key is encrypted using the symmetric key. Towards a Trusted Virtual Machine Launch Mechanism 93On the cloud management server, the root key of the TPM will be stored. The key management center in the cloud The Usbkey is given to the user by the Usbkey administrator. The user accesses the cloud administration center and submits an application for a virtual machine.

For the user, the cloud management center builds a virtual computer. A host is used to execute the encrypted virtual machine image. Meanwhile, TPM key migration will transfer the symmetric key to the host. After that, the local TPM will safeguard you. The picture encryption in VMMThe picture will be decrypted using the migrated symmetric key by the decryption module. Both the VM and the user will cooperate. Authenticate using the Usbkey's symmetric key and the migrated key. When the user logs onto the virtual machine. The attestation server will interact with the trust inquiry module in VM to get the VM's measured result. Then On the VM's desktop, the trusted status will be shown. Detailed Planning Image encryption decryption, measurement, attestation, and a security-enhanced method based on TPM are all included in TLVM. The in-depth analysis the following is a description of their design. VM Image Encryption Mechanism Unauthorized users may launch a virtual machine's images in the cloud.

Administrators may, for example, transfer a virtual machine image to another computer. Start the virtual computer outside of trusted domains. In order to be safe, the most effective technique for preventing an illegal start of a user's virtual machine is complete virtualization. The picture is encrypted on the computer drive, making it impossible to retrieve it. For unregistered users however, it is clear that this is a time-consuming procedure. ToWe simply encrypt the essential data to strike a balance between security and speed. A virtual machine image's disk metadata. We could do this for a standard disk file. The master boot records (MBR), Boot, and certain logic partitions should all be encrypted.

2.1. Application:

However, inSome virtual computers in a cloud environment may have the same MBR or boot. ItIt's simple to clone a VM and use it to target other VMs. As a result, we've created an image file. The encryption is dependent on the file system and the user's settings. We started with the basics. Obtain the TPM-protected symmetric key of the user, and get the partitionand get the user's encryption from the MBR and file system type informationconfiguration. Finally, we

encrypt the configuration file and save it. Then encrypt file system key information, such as index structure. The following is a summary of the VM image encryption process.

Decrypt the symmetric key that has been transferred to the host where the virtual machine is running. When the VM starts, the TPM's SRK in the host raises an objection. Valuesncryption Mechanism Unauthorized users may launch a virtual machine's images in the cloud. Users. Administrators may, for example, transfer a virtual machine image to another computer. Start the virtual computer outside of trusted domains. In order to be safe, the most effective technique for preventing an illegal start of a user's virtual machine is complete virtualization. The picture is encrypted on the computer drive , making it impossible to retrieve it. for unregistered users However, it is clear that this is a time-consuming procedure. ToWe simply encrypt the essential data to strike a balance between security and speed.

We could do this for a standard disk file.The master boot record (MBR), Boot, and certain logic partitions should all be encrypted. However, in some virtual computers in a cloud environment may have the same MBR or boot. ItIt's simple to clone a VM and use it to target other VMs. As a result, we've created an image file. The encryption is dependent on the file system and the user's settings. We started with the basics. Obtain the TPM-protected symmetric key of the user, and get the partitionand get the user's encryption from the MBR and file system type informationconfiguration. Finally, we encrypt the configuration file and save it.Then encrypt file system key information, such as index structureThe following is a summary of the VM image encryption process: Decrypt the symmetric key that has been transferred to the host where the virtual machine is running.When the VM starts, the TPM's SRK in the host raises an objection. Get the file system for the partition and the operating system is located at the end of the MBR. We may get information about the partitions, such as as well as the original location, size, and file system Load the user's crypto settings. Every virtual machine (VM) has a crypto configuration that is secured by the VM's symmetric key. Every business is in operation. There is a default setup for the system [6].

2.2. Working:

Examine the picture file to see whether it has been encrypted. We've created a flag to identify the picture file's crypto state in order to prevent repeated encryption. IThe picture file has been encrypted, and the crypto procedure will begin shortly. Be shattered Encrypt a configuration file's included file. In order to maintain equilibrium, we've developed elastic encryption for performance and security. The Some kernel files that are ubiquitous for the same operating system are included in the configuration. It must contain the boot, registry, bootmbr, ntldr, and other files for Windows 7.boot.ini, winlog.exe, and a few more crucial items Users can't see these files since they're hidden. Additionally, users may encrypt additional critical data. For some file systems, encrypt the import partition. Various file systemsFiles are organized in a variety of ways. For a Linux system, we look at everything.

Partition, then obtain the partition's fundamental information from the super blockthen go through all of the block groupings Following that, we encrypt the group and block. Every block group has its own bitmap,. Because the picture files are large [7].

We just rewrite the encrypt portion to the picture file since they are often big. The VM Measurement Mechanism the VM measuring mechanism determines the integrity of a VM.before the event begins. The term "system integrity" refers to the state of a system's integrity. To determine In reality, a whole system is extremely costly. Associating is one effective method. The integrity semantics for a few key files we measure in our mechanism.the most essential files from several systems, as well as certain user-defined files Fore measured the boot, grub, kernel, kernel modules, and binaries on Linux computers. There are two types of libraries: shared libraries and dynamic libraries. We should assess the performance of Linux users [8].

Send and validate the measurement by calling the attestation client module.values. Remote attestation does the integrity verification of a system. It can prove whether system data is tampered with. It also provides a credible platform status report to a verifier. For remote attestation, TPM is the trusted root of the report. It helps ensure the report deriving from the current integrity measure values. There are some differences between the remote attestation of VM and the general remote attestation protocol [10].

Attestation client receives them, and then triggers the attestation server to send a nonce to the attestation client. After the attestation client gets the nonce, it uses SHA1 algorithm to calculate a hash value of the measurement value, then loads a private signing key from TPM to sign the hash value, forming an integrity report. The report includes nonce, measurement value, hash value, signature value and some other information about the VM. Finally, the attestation client sends the integrity report and measurement log to the attestation server. The attestation server checks nonce, verifies hash and signature, and then judges the platform’s credibility by comparing the signature and the expected value [9].

3. CONCLUSION:

We presented a trusted launch solution for virtual machines in this article, which comprises four systematic methods to secure virtual machines in clouds: image encryption, measurement, attestation, and security-enhanced authentication. Unauthorized users won't be able to start a virtual machine if the images are encrypted. A VM's integrity may be protected via measurement and attestation mechanisms. Two-way authentication between a user and a virtual machine is possible with security-enhanced authentication. The methods provide a methodical approach to starting a virtual machine in a safe manner. A proof-of-concept implementation of our method is also discussed. The results of our tests show that our technology can secure the whole launch process of a virtual machine.

Decrypting the VM imp takes approximately 4.717 seconds in total, including 3.852 seconds for decrypting the key using TPM SRK, 0.223 seconds for storing the temp file, 0.267 seconds for decrypting the img disk file system, and 0.368 seconds for decrypting the file provided in the configuration file. Mounting the image file took 0.186 seconds, measuring the kernel took 0.241 seconds, measuring dynamic link libraries took approximately 0.432 seconds, measuring boot files took 0.164 seconds, and measuring drivers took 0.459 seconds.

The attestation time is about 6.277 seconds. It takes 0.569 seconds to generate measurement report-based measurement files. It will take 3.872 seconds to sign the measurement hash value. It takes 0.684 seconds to verify the signature and compare the value to the baseline values. The time spent communicating with the attestation server remains. The time it takes to authenticate with a USBkey is approximately 7.663 seconds, which includes nonce creation time, communication time, and encryption decryption time

REFERENCE

[1] Z. Yu, W. Zhang, and H. Dai, "A Trusted Architecture for Virtual Machines on Cloud Servers with Trusted Platform Module and Certificate Authority," *J. Signal Process. Syst.*, 2017.

[2] J. Wang *et al.*, "Towards a trusted launch mechanism for virtual machines in cloud computing," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2014.

[3] M. A. Ajay Kumara and C. D. Jaidhar, "Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment," in *2015 International Conference on Telematics and Future Generation Networks, TAFGEN 2015*, 2015.

[4] H. Jin, G. Cheng, D. Zou, and X. Zhang, "Cherub: Fine-grained application protection with on-demand virtualization," *Comput. Math. with Appl.*, 2013.

[5] H. Maziku, "Towards infrastructure based software defined security," *ProQuest Diss. Theses*, 2016.

[6] Z. Yu, Q. Wang, W. Zhang, and H. Dai, "A cloud certificate authority architecture for virtual machines with trusted platform module," in *Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, HPCC-CSS-ICESS 2015*, 2015.

[7] S. Jin, J. Ahn, S. Cha, and J. Huh, "Architectural support for secure virtualization under a vulnerable hypervisor," in *Proceedings of the Annual International Symposium on Microarchitecture, MICRO*, 2011.

[8] J. H. Huh *et al.*, "An empirical study on the software integrity of virtual appliances: Are you really getting what you paid for?," in *ASIA CCS 2013 - Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, 2013.

[9] O. Yevsieieva and S. M. Helalat, "Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment," in *2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings*, 2017.

[10] C. Maurice, C. Neumann, O. Heen, and A. Francillon, "Confidentiality issues on a gpu in a virtualized environment," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.