Secure Virtual Machine Migration (SV2M) in Cloud Federation

Muhammad Awais Shibli, Naveed Ahmad, Ayesha Kanwal and Abdul Ghafoor
National University of Sciences and Technology,
School of Electrical Engineering and Computer Science, Islamabad, Pakistan

Keywords: Virtualization, Virtual Machine, Secure Migration, Cloud Computing.

Abstract: Virtual Machine (VM) migration is mainly used for providing high availability, hardware maintenance, workload balancing and fault takeover in Cloud environment. However, it is susceptible to active and passive security attacks during migration process, which makes IT industry hesitant to accept this feature in Cloud. Compromising the VM migration process may result in DOS attacks, loss of data integrity and confidentiality. To cater different attacks such as unauthorized access to images and injecting malicious code on VM disk images, Cloud Providers store images in encrypted form. Therefore, security of VM migration along encrypted disk images keys becomes necessary. Previously, research focus was on the performance of VM migration, leaving security aspects of migration process completely explored. This paper proposes a comprehensive solution for Secure VM Migration (SV2M) in Cloud environment, which ensures authorization, mutual authentication, confidentiality, replay protection, integrity and non-repudiation with minimal changes in existing infrastructure. We have extended the key manager of Cloud provider and introduced new features for management and storage of keys involved in our proposed SV2M solution. In addition to this, we have integrated the proposed solution with OpenStack, which is an open source Cloud platform used by large community for research in Cloud computing. We also evaluated the security of SV2M system using well known automatic protocol verification tool AVISPA.

1 INTRODUCTION

Cloud technology has changed the IT industry in last decade and it is gaining attention in enterprises because of scalability, increased efficiency, lower infrastructural cost and better utilization of hardware resources. It enables ubiquitous, handy, on-demand access to a shared pool of configurable computing resources (e.g. applications, networks, storage and services) that can be quickly provisioned and released with minimal management effort or service provider involvement (Hashizume et al. 2013; Mell 2013). The delivery models of Cloud technology are, Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). From the Cloud service provider (CSP) perspective, both delivery models SaaS and PaaS are dependent on IaaS for their services. Similarly any security violation in IaaS delivery model will have an effect on SaaS and PaaS security and vice versa (Hashizume et al. 2013).

Cloud computing is a combination of several other technologies such as virtualization, Service Oriented Architecture (SOA) and web. Virtualization is one of the most critical technologies of Cloud and it enables the abstraction of hardware resources for the purpose of improved and better hardware utilization leads to reduce operational and investment costs. CSP allocates VM to consumers from pool of virtualized computing resources such as storage, network, processing and others in IaaS delivery model. Security constraints of virtualization technology are also inherited in the Cloud along with their benefits. VM security becomes critical for overall security of Cloud because virtualization introduces new attacks and challenges (Hashizume et al.2013;Mell 2013; Vaidya 2009).

VM migration or mobility is the key feature of virtualization technology which is used to provide hardware/system maintenance, work load balancing, and transparent management in conventional data centers as well as in Cloud infrastructure (Anala et al. 2012). Apart from providing major features, VM migration provided by VMware,XEN and Hyper-V hypervisors is prone to security risks. XenMotion, which is migration module of Xen, exposes the sensitive and critical information of guest OS

Awais Shibli M., Ahmad N., Kanwal A. and Ghafoor A..
Secure Virtual Machine Migration (SV2M) in Cloud Federation.
DOI: 10.5220/0005057103440349
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 344-349
ISBN: 978-989-758-045-1

because migration does not provide security features such as confidentiality and authentication (Cooke et al. 2008). Currently, CSPs are using different security mechanisms for securing VMs in Cloud such as encryption of disk images to counter attacks (Kazim et al. 2013). However, VM migration with metadata (keys of encrypted disk mages) is not secure because of unavailability of strong security features in hypervisors.VM migration without security becomes single point of failure for Cloud environment because intruder can inject malicious code or modify the VM content. Successful attack on migration process may cause denial of service (DOS), loss of data integrity and confidentiality in transmitted VM (Cooke et al. 2008).

The latest research on resource migration is performance oriented, therefore, security issues have not received much attention. This paper presents the holistic solution on Securing VM migration in Cloud. Our proposed solution provides mutual authentication between the CSPs, authorization, confidentiality, integrity, replay resistance and non-repudiation. After successful migration of VM, CSP updates key manager with encrypted disk images keys (EIK). In addition, load monitoring module is used to continuously monitor resources on sender/receiver CSPs and intimate them for the acceptance/rejection of VM migration requests. The remaining paper is organized as follows: section 2 presents background of VM migration and its different types. Section 3 presents related and existing work on VM migration security. Section 4 presents proposed architecture and workflow of secure VM migration process. Section 5 presents the verification of protocol using AVISPA and Section 6 concludes the paper along with future work directions.

2 BACKGROUND

This section provides some background information about VM migration and its different types which are supported by well-known hypervisors. Migration is the useful feature of Virtualization technology which is used to transfer a VM from one physical server to another or from one data centre to another. This feature provides efficient system maintenance, load balancing and proactive fault tolerance in enterprises infrastructures (Anala et al. 2012; Cooke et al.2008). VM migration is also used in Cloud Federation to provide Cloud bursting feature (Kenneth et al. 2011).

2.1 Types of VM Migration

VM migration is categorized into cold and hot migration. In cold migration, also known as offline migration, first VM is shutdown and then transferred to other host or data centre (VMware Migrating VM). In hot migration, VM is transferred without shutting down the machine and it is used to minimize the downtime. Both live and suspended/paused VM migrations are placed in this category. Live migration is defined as transfers of running VMs from one physical server to another with minimum downtime and without interrupting the services running in VM (Anala et al. 2012). Live migration is further classified into memory migration and block/storage migration. In memory migration, only contents of volatile memory of VM are migrated and in block migration, the storage of VM is also migrated along with memory and it takes longer as compared to memory migration. However, in suspended/pause migration technique, contents of VM is stored in disk or in memory (RAM) respectively before transfer from one Cloud to another (OpenStack documentation, pausing & suspending instances 2013).

3 RELATED WORK

This section discusses in more detail some of the existing solutions or approaches for secure VM migration in Cloud environment. Many existing solutions are using Trusted Platform Module (TPM) in their solution and only support offline migration.TPM dependent solutions require changes in software (virtualization of TPM in hypervisor) and hardware of current Cloud infrastructure. Approaches which provide security in live VM migration are not comprehensive and do not fulfil all the essential security features (such as Mutual Authentication, Authorization, Replay Resistance , Confidentiality and Integrity of VM contents during migration process and Non-Repudiation) of Live migration process (Anala et al. 2012; Zhang et al. 2012).

Isolated/segregated migration uses Virtual LAN (VLAN) to isolate migration traffic from other network traffic because it reduces the risk of exposure. However, it does not provide any security feature and cost of VLAN management is also linked with population of VM's (Anala et al. 2012; OpenStack security guide, 2013). In Network Security Engine-Hypervisor based approach, firewall and IDS/IPS functionalities become part of

hypervisor for protection against intrusions. However, it does not provide security features during the VM migration process (Anala et al. 2012). In Policy or Role based secure migration approach, only offline VM migration is supported and it requires changes at software and hardware level for linking in existing infrastructure (Anala et al. 2012; Wang et al. 2010). Security requirements such as replay resistance is not part of this approach.

Secure VM-vTPM migration protocol provides mutual authentication and establishes secure session for subsequent communication. However, this approach does not support live migration and keys of vTPM are also stored outside the TPM, therefore prone to leakage and unauthorized modification (Anala,et al. 2012; Danev et al. 2011). Another such approach includes vTPM migration protocol, where both parties mutually authenticate each other and then property based remote attestation is performed by source host to verify the integrity of destination. Key exchange is performed using Diffie-Hellman which is used to achieve confidentiality during migration process. This approach only supports offline migration and vTPM state is also migrated (Zhang et al. 2012). In this paper, author (Kenneth et al 2011) proposed solution that uses proxy and secure shell (SSH) to ensure security while VM migration. Proxies are used to restrict access to end nodes which are involved in VM mobility and SSH tunnel is established between both proxies to achieve confidentiality. However it does not provide authorization and non-repudiation security features and port forwarding is require on all intermediate devices and firewalls (Kenneth et al 2011).

RSA with secure shell (SSL) based approach provides authentication, encryption, and reply resistance during migration process. For authentication, it requires public keys of all other hypervisors for VM migration however it includes the difficulties of public key management (Patil & Patil 2012). Fengzhe et al. (2008) proposed Protection Aegis for Live Migration of VM's using customized Virtual Machine Monitor called VMM enforced protection system which provides security to running processes in VM. In this approach, protected memory pages also transfer as metadata along VM. Furthermore it does not provide authentication and authorization security features.

4 PROPOSED SYSTEM

Our proposed solution provides protection against active and passive attacks during the migration process. The solution introduces strong security features such as mutual authentication between CSPs, authorization before initiation of migration operation, confidentiality, integrity, replay resistance and non repudiation. The architecture of proposed system is shown in Figure 1.

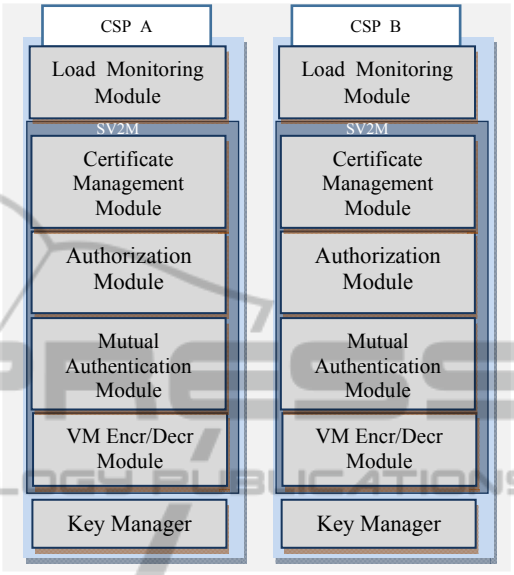

Figure 1: Proposed Architecture of SV2M system.

Proposed SV2M solution encompasses different components. At its core part is SV2M module, which is further divided into sub modules such as i) Certificate Management Module (CMM) ii) Authorization Module (AZM) iii) Mutual Authentication Module (MAM) iv) Encryption and Decryption Module (EDM). Other components are Load Monitoring Module (LMM) for continuous monitoring of Cloud resource and Key Manager (KM) for storing the keys, which include encrypted disk image keys (EIK) and VM encryption keys (VMK). All these modules communicate with other components of Cloud platform. The detailed functionalities of each module are described below.

4.1 SV2M Module

It consists of four sub modules: CMM, AZM, MAM and EDM, each described in following subsections.

4.1.1 Certificate Management Module

This module is used to generate certificate request to Trusted Third Party for CSP and also store certificate in the Cloud platform. This certificate is later used by the authentication module for entity authentication using FIPS-196.

4.1.2 Authorization Module

This module checks the authorization of current user/operator before initiating VM migration operation. It can be initiated by those roles which are allowed by Cloud administrator.

4.1.3 Mutual Authentication Module

This module ensures that source and destination CSPs are ready to perform migration. In this module, CSPs send X.509 certificates to each other and perform authentication. We are using FIPS-196 to achieve mutual authenticity between CSPs before VM transfer (entity authentication using Fips196, 1997).

4.1.4 VM Encryption & Decryption Module

After successful mutual authentication between CSP's, the next step is encryption and digital signature of suspended/paused VM at sender CSP end. We are using XML Encryption and Signature in this module. First of all, XML signature of suspended VM is created and signed with private key (Priv_KA) of Cloud A. In the next step, encryption key (VMK) for suspended VM is retrieved from key manager and used for XML Encryption of VM using AES algorithm. In final step, both VMK and EIK are encrypted using the Public Key (Pub_KB) of Cloud Band transferred along XML encryption and signature of VM, as shown in Figure 2.

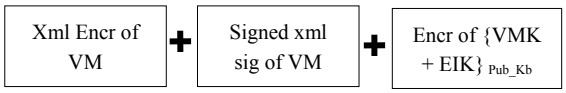

Figure 2: Encryption of message at sender side.

After the encrypted VM is received, the decryption module extracts the VMK and EIK using the private key (Priv_KB) of Cloud B. The EI key of received VM is stored in the Key Manager, whereas VMK is used to decrypt the migrated VM. For XML signature verification, ED module decrypt the signed XML signature of VM using Public key of Cloud A (Pub_KA) and compare it with newly created XML signature of decrypted VM, as shown in Figure 3. After successful verification, suspended VM is resumed on receiver Cloud for providing services.

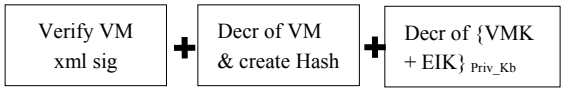

Figure 3: Decryption of message at receiver side.

4.2 Key Manager

Key Manager provides key management such as generation, their secure storage, update and deletion. CSP uses KM for server side encryption such as Object Storage transparent encryption by Google and Amazon (OpenStack, Key Manager, 2013). CSP also use it for storage of encrypted disk images keys (EIK) which are used to protect disk images in Cloud repositories (Kazim et al. 2013 ;Oleg Gelbukh 2012 ;HighCloud Security, Encrypt VM images 2011; HighCloud Security 2013). It is also used for generation and storage of VM encryption keys (VMK) for ED module. In secure migration module, EIK and VMK are transferred to the receiver Cloud Provider along with encrypted VM. After successful resumption of VM, disk image key (EIK) is stored on the key manager at the receiver end.

4.3 Load Monitoring Module

This module is used to monitor the Cloud resources which include the unused random access memory (RAM), storage and virtual CPU (vCPU) etc. and linked to SV2M module. It intimates the source Cloud (Cloud A) operator about the migration of VM due to unavailability of resources for new VMs. It also intimates the destination or receiver Cloud (Cloud B) whether it can accept or reject the VM migration request based on available resources.

Complete workflow of proposed system is shown in Figure 4. Description of each step is given below.

1 As a first step, source & destination CSPs request trusted CA for certificates. These certificates and their private keys are stored in Cloud platform.
2 In this step, AZM checks whether the Cloud operator can initiate request for VM migration operation or not.
3 After the successful authorization, CSP A initiates VM migration request toward CSP B. Request will be accepted by CSP if enough unused resources are available for migrated VM. Acceptance and rejection of migration request depends upon Load monitoring module because it intimates the SV2M module about the available resources. In this step, both CSPs mutually authenticate each other using FIPS196 entity authentication. Both parties share their X-509 certificate in this mechanism.
4 Cloud providers have repositories of VM disk images which are encrypted to protect against offline attacks while at rest. Whenever the

customer requests for VM, CSP first decrypt the disk image using key (EIK) which is stored in key manager and run it using hypervisors such as KVM/VMware on Cloud. EI key is also migrated along with the suspended VM. Therefore, Cloud Provider A first suspends running VM and retrieve corresponding EIK. XML signature of suspended VM are created and signed by the sender. XML encryption is also performed on VM using key VMK. Finally, VMK& EIK are also encrypted using the public key of Cloud B and sent to Cloud B.

5 When Cloud B receives the encrypted VM with signatures and encrypted Keys (EIK &VMK), first it decrypts the encrypted keys using Private Key of Cloud B. EIK is stored in the key manager and VMK is used for decryption of encrypted VM. In parallel, Cloud B also decrypts the XML signatures of VM using Public key of Cloud A and compare it with XML signature of received VM. Migrated VM is resumed on Cloud B hypervisor after successful verification.

6 Cloud B acknowledges the Cloud A after successful execution of VM so that it is removed from sender CSP.

5 AVISPA VERIFICATION

AVISPA is a web based automated tool for the validation of security protocols and application. It uses a formal language known as High Level Protocol Specification Language (HLPSL) for the specification of protocols and their security goals and integrates different back-ends such as SATMC, TA4SP ,CL-AtSe and OFMC for implementation of range of analysis techniques. It is assumed in analysis that the protocol meets cryptography and also network over message exchanged is controlled by Dolev-Yao intruder as an active intruder (AVISPA, User manual 2006).

AVISPA analysed the protocol against security goals such as secrecy of key, weak/strong authentication. We analysed the secure migration protocol against security requirements such as strong authentication (G1, G5),Non-repudiation (G18) secrecy (G12), integrity (G2), reply protection (G3) (AVISPA, User manual 2006). The result of back end analysis techniques against abovementioned security properties is shown in Figure 5.

The output summary of AVISPA indicates that a SV2M protocol is safe under analysis of back-ends and no attack is found on it.

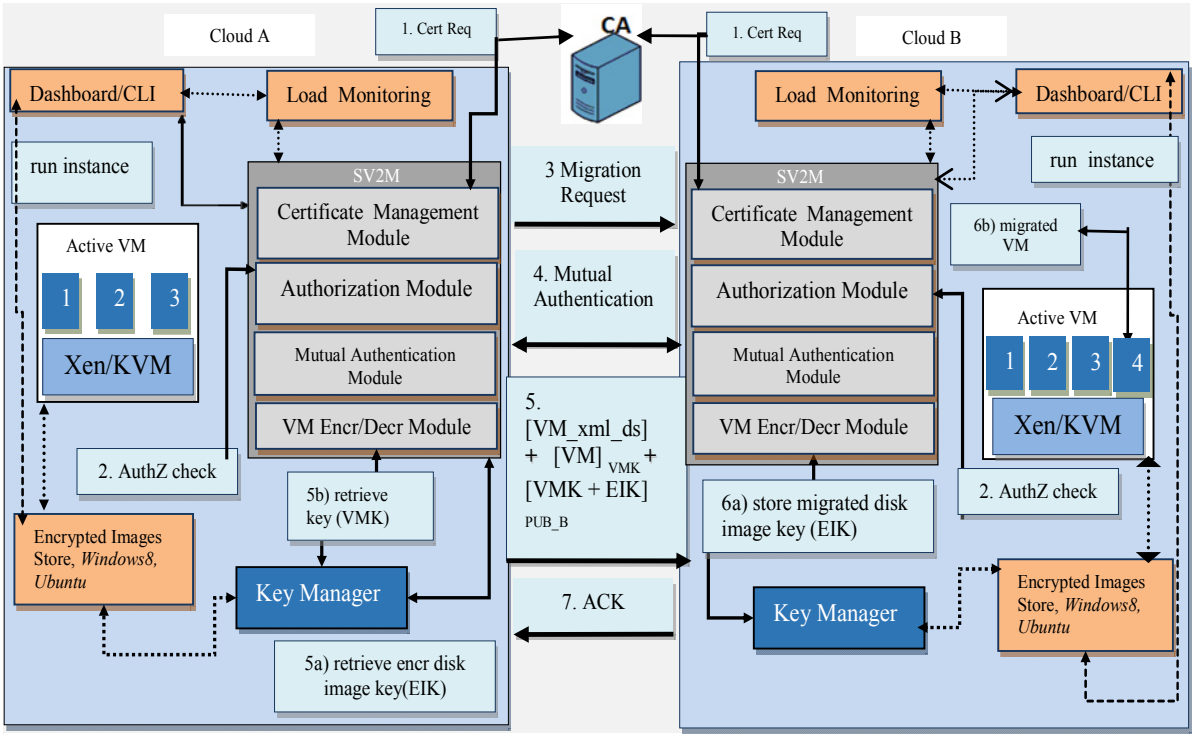

Figure 4: Overall workflow of SV2M module.

6 CONCLUSIONS

VM migration is valuable feature for Cloud environment; however, it also introduces new security concerns such as illegal modification of VM content during migration. In this paper we proposed a holistic solution for VM migration which provides strong security features such as mutual authentication between Cloud Providers, authorization of migration operation, confidentiality and integrity of VM content, replay resistance and non-repudiation of source Cloud. Our solution requires minimum changes in existing Cloud infrastructures because it is not dependent on any hardware chip (TPM). In future, we will evaluate its performance with other existing solutions and decrease the encryption/decryption time of SV2M module. Security aspects of receiver Cloud after successful migration is also potential research area. Cloud providers are also using snapshots for instance migration; therefore, security in snapshot migration is our future goal.

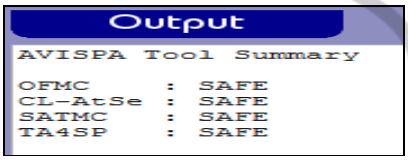

Figure 5: Result summary of AVISPA.

REFERENCES

K. Hashizume, Fernández 2013. An analysis of security issues for cloud computing In *Journal of Internet Services and Applications Production*.

P. Mell, Grance,2013. 'The NIST definition of cloud computing". NIST, Special Publication 800–145

V. Vaidya, 2009. Virtualization vulnerabilities and threats :<http://www.redcannon.com/vDefense/VM_secuity_ wp.pdf >.

J. Shetty, Anala R, Shobha 2012. A survey on techniques of secure live migration of virtual machine. In *Intl Journal of Computer Applications, vol. 39,no.12.*

J. Oberheide, E. Cooke and F. Jahanian, 2008. Empirical exploitation of live VM migration In *Proceeding of BlackHat DC convention*

M. Kazim, Rahat Masood & M. Awais,2013. Securing the vm images in cloud In *Proceedings of the 6th International Conference on Security of Information and Networks.*

K. Nagin, D. Hadas, Z. Dubitzky, and Schour, 2011.Inter-cloud mobility of virtual machines. In *Intl Conference on Systems and Storage,Haifa, Israel*.

Migrating VM Available from <http ://pubs . vmware.com /vsphere-4-esxvcenter/index.jsp?topic=/com vmware.vsphere.dcadmin.doc_41/vsp_dc_admin_guide/migrating_virtual_machines/c_migrating_virtual_machines>

Pausing and Suspending Instances ,2013. Available from <http://docs.openstack.org/grizzly/openstack-compute/admin/content/pausing-and-suspending-instances.html>

X. Wan, X. Zhang and J.Zhu, 2012. An improved vTPM migration protocol based trusted channel. In *Conf erence on Systems and Informatics, pp. 871-875.*

OpenStack Security guide, 2013.Available from: <ht tp://docs.openstack.org/security-guide/security guide.pdf>

W. Wang, Y. Zhang, B. Lin and K.Miao,2010.Secured VM migration in personal cloud. In *2nd Intl Conference on Computer Engineering &Tech*

B. Danev, R. J. Masti, and S. Capkun 2011, Orlando, Florida. Enabling secure VM-vTPM migration in private clouds. In *Proceedings of the 27th Annual Computer Security Applications Conference.*

Y. Chen, Q. Shen, P. Sun, Y. Li 2012. Reliable migration module in trusted cloud based on security level design and implementation. In *International Parallel and Distributed Processing Symposium Workshops &PhD Forum.*

V. P. Patil and G.A. Patil, 2012. Migrating process and vm in the cloud: In *International Journal of Advanced Computer Science and Information Technology , vol. 1, pp. 11-19.*

Zhang, Y. Huang, 2008.PALM: security preserving VM live migration for systems with VMM-enforced protection. In *Third Asia-Pacific Trusted Infrastructure Technologies Conference.*

Key Manager, 2013.Availabe from:<https://wiki .openstack.org/wiki/KeyManager>

Oleg Gelbukh, 2012, OpenStack Swift Available from: <http://www.mirantis.com/blog/ openstack-swift-encryption-architecture/>

HighCloud Security, Encrypt VM images, 2011.Available from: <http://www.net-security.org/secworld.php ?id=11825>

HighCloud Security 2013. Available from:<http://www . highcloudsecurity.com/blog/secure-vmbackups-w hat-is-different-and-why-should-you-care/>

Entity Authentication using PKCS, FIPS Publication 196 , 1997.

AVISPA User Manual,2006Available from: <http://www. avispa-project.org/p ackage/user-manual.pdf>