Secure Live Virtual Machine Migration in Cloud Computing

[1]Prashant Sahatiya, [2]Harshal Shah

[1]M.Tech-CE Student, [2]Professor
[1-2]Department of Computer Science & Engineering
[1-2]Parul Institute of Engineering & Technology, Vadodara, India

***Abstract*—** The center of Cloud processing incorporates virtualization of equipment assets, for example, stockpiling, system and memory gave through virtual machines. The live relocation of these VMs is acquainted with get different advantages which chiefly incorporate high accessibility, equipment support, blame takeover and outstanding task at hand adjusting. Other than different offices of the virtual machine relocation, it is powerless to extreme safety dangers amid movement process because of which the business is reluctant to acknowledge it. The exploration done till date is on the execution of movement process; while the safety perspectives in relocation are not completely investigated. We have completed a broad review to research the vulnerabilities, dangers and conceivable assaults on the live virtual machine migration. Besides, we have recognized security necessities for safe virtual machine relocation and exhibited a nitty gritty examination of current arrangements based on these security prerequisites. At last, impediments in the current arrangements are displayed.

Keywords*— *Virtualization, Live Virtual Machine Migration, Cloud Computing, Cloud Security, Infrastructure as a Security (IaaS)

I. INTRODUCTION

Distributed computing is getting thought in nearly nothing and medium undertakings (SME's) in light of lower infrastructural cost. It engages inescapable, worthwhile, on-ask for arrange access to a common pool of configurable figuring resources (e.g., frameworks, servers, storing, applications, and organizations) that can be immediately provisioned and released with unimportant organization effort or expert association collaboration [1, 2]. Circulated figuring gives organizations by methods for Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) transport models. SaaS is an item transport show in which applications live on cloud authority association (CSP) and are open for its client by methods for a web program (e.g., Google docs). PaaS show implies the movement of working structures and related gadgets over the web. A purchaser sends his application on the CSP without presenting any stage or gadget on their adjacent machines. In IaaS movement illustrate, CSP re-fitting the getting ready, storing, framework and all other enrolling resources as VM's.

Distributed computing is giving various favorable circumstances to SME's, in any case there are so far various basic obstructions in its gathering. The security of data and information in Cloud is the crucial stress of any affiliation. Security hindrances in these customary progressions are in like manner gained in the general security of Cloud nearby their favorable circumstances. As Cloud structure includes immense scale, dispersed, heterogeneous and absolutely virtualized resources, thusly the regular security frameworks are lacking for this condition. In SaaS movement show, the customer has very less control over the benefits; subsequently the CSP is responsible for managing the required security framework. In SaaS movement illustrate, the customer has less expert over the benefits consequently the heaviness of security lies on CSP. While the PaaS movement show offers progressively significant customer control as a diverge from SaaS, along these lines both CSP and customer are accountable for resources security. IaaS offers progressively critical customer direction over security when appeared differently in relation to the PaaS or SaaS models. We need to understand the associations and conditions between the three referenced Cloud movement models. he PaaS and SaaS models are dependent on IaaS for their organizations, in this manner any break in IaaS model will in like manner influence the security of both PaaS and SaaS and the a different way. Virtualization is principle advancement in IaaS movement show where Cloud Service Provider gives a mutual pool of limit, mastermind, and other figuring resources as VM. Regardless, other than the diverse favorable circumstances of virtualization it has in like manner introduced new open entryways for aggressors [1, 2]. Subsequently VM security ends up fundamental for as a rule wellbeing of IaaS illustrate.

In IaaS show, CSP disseminates advantages for purchasers using VM which is a middle fragment of Cloud figuring. As such, it is basic to think about the security of Virtual Machine in Cloud space. Virtualization gives distinctive focal points in Cloud anyway it also raises security risks that can impact the Cloud condition. The noteworthy virtualization express vulnerabilities and risks that must be taken in perception in Cloud join (I) VM poaching (ii) the VM bouncing (iii) and unbound live VM development. In VM poaching strike, movement. In VM poaching attack, guest working structure (OS) involves more CPU, memory or some other figuring assets assigned to it against the other visitor OS running in the equivalent hypervisor. VM ricocheting attack, abuses the vulnerabilities of Hypervisors that empowers harmful code to evade VM protections and expansion control to some other VM. Live VM migration instrument used to trade VM beginning with one physical server then onto the following with least downtime however separated or suspended VM development grows the downtime. It gives extraordinary weight modifying, gear/structure support, high openness organizations, direct versatility and blended organization. The unbound live VM migration conceivably opens up the security risks and presentation for the moved VM just as for exchange guests OSes running on that Physical Server [3, 4, 5].

In such manner, we have completed a broad overview of live VM relocation, distinguished the vital vulnerabilities in movement module just as in live VM movement process. Besides, found the different dangers found in writing identified with the VM relocation in Cloud processing. We have likewise recognized the security necessities for VM movement and examination of existing arrangements based on these distinguished prerequisites. Moreover, constraints of existing arrangements and methodologies are additionally investigated. Whatever is left of the paper is sorted out as pursues: segment II presents synopsis of the subjects that are examined in the VM relocation writing. Segment III exhibits the recognized vulnerabilities and dangers on live VM movement process. Segment IV contains the investigation of existing arrangements and restrictions of VM Migration procedure and segments. Segment V contains the proposed architecture for secure live VM migration and segment VI finishes up the paper alongside future research headings.

II. Review of Literature

We have outlined the writing audit in the Table I. We distinguished that the majority of the papers talked about the dangers and vulnerabilities in live VM movement. As appeared in the Table I, proposed arrangements for the most part focus on the disconnected VM movement and though live VM relocation has not gotten much consideration. In addition security prerequisites for secure live VM relocation process are likewise examined. Besides, it is additionally examined that unreliable live VM movement brings security hazard up in IaaS model of Cloud Computing. Dangers and vulnerabilities of movement procedure will likewise affect the security of IaaS demonstrate.

Table I Synopsis of Literature on VM Relocation

Topics/ References	**1**	**3**	**6**	**7**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Vulnerabilities	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Threats / Attacks	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓
Mechanism for Secure offline VM migration	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗
Mechanism for secure live VM migration	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓
IaaS security	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Security Requirements	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗

III. Recognized Dangers and Vulnerabilities in Live VM Movement

Jon et al [3] has experimentally shown that live VM movement process is inclined to dynamic and uninvolved assaults. Assaults on live VM process are classified into control plane, information plane and relocation module classes.

A. Control Plane

Hypervisor exercises, for instance, initiation and the leading group of live VM development must be affirmed and safe against modifying. In addition, affirmation against satirizing and replays ambush should be given. A nonattendance of security in the control plane may empower an attacker to abuse live movement action in different ways:

1. Denial-of-Service (DoS) assault: Attacker will make many VM's on the host OS only to over-trouble the host OS, which won't in all probability recognize any increasingly migrated VM's.
2. Superfluous movement of VM: Assailant will over-load the host OS by unneeded VM's. This will compel execution of the dynamic weight changing feature, which will ensure development of some VMs to alter the stack.
3. Approaching Migration Control: The attacker can begin an unapproved migration request, so VM can be moved from secure source physical machine to an exchanged off aggressor machine. This may result in aggressor increasing full power on the legitimate VM.
4. Active Migration Control: The aggressor can begin the VM development and can make the maltreatment of the cloud resources which can incite disillusionment of the VM.
5. Disturb the ordinary tasks of the VM: An attacker may move a VM beginning with one host then onto the following host with no goal however to meddle with the exercises of the VM.
6. Assault on VMM and VM: Assailant will move a VM that has a pernicious code to a host server that has the goal VM. This code will exchange information with the VMM and the goal VM through a hidden channel. This channel will deal the arrangement of the host server by spilling center around VMs' information.
7. Promoting for false asset: Aggressor plugs false resource openness for the goal VM. For example, publicizing that there is a generous number of unused CPU cycles. This results in migration of the VM's to an exchanged off hypervisor moving VM. The assailant gets information from the VM's moving memory (e.g., passwords, keys, application data, getting packages that are starting at now checked, messages that have tricky data will be gotten, etc.) [18].

B. Data Plane

Live VM Migration happens in this plane, memory substance, for example, portion states and application information exchange starting with one physical server then onto the next. Aggressor can utilize ARP ridiculing or DNS harming strategies to dispatch man in the middle (MITM) assault on unreliable correspondence channel. This presents dynamic and inactive assaults amid the movement procedure. Thusly secure and ensured channel must be use to limit snooping and altering endeavours on relocation information. Consequently, an assailant may put himself in the trans-mission channel to play out a man-in-the-middle assault utilizing any of the procedures: Address Resolution Protocol (ARP) parodying, Domain Name System (DNS) harming, or course commandeering [18]. Man-in-the-middle assault can be one of the two kinds of assaults - inactive and dynamic:

1. Passive Attack: Aggressor watches the transmission channel and other framework streams used to get the information of migrating VM. The aggressor gets information from the VM's migrating memory (e.g., passwords, keys, application data, getting packs that are currently checked, messages that have fragile data will be gotten, etc.) [18].

2. Active attack: This assault is the most genuine assault in which the aggressor controls the memory substance (e.g., validation administration and pluggable verification module in live relocation) of moving VM's [18].

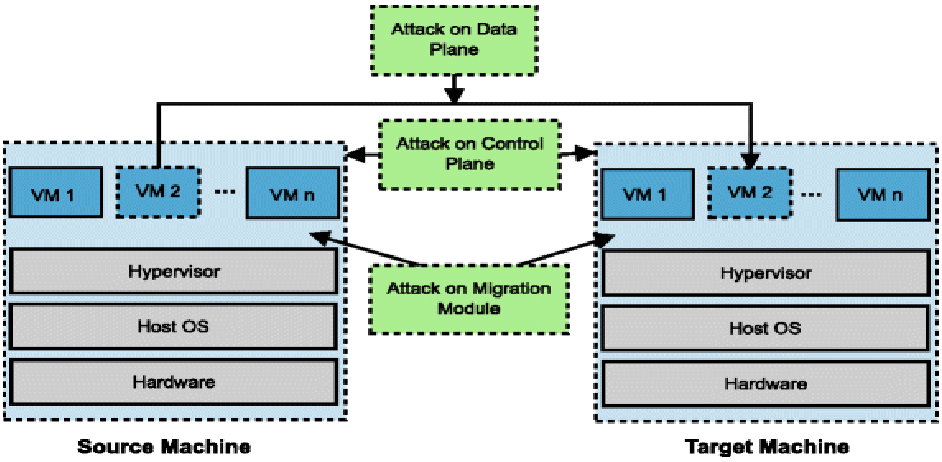


Figure 1Possible attacks during Live VM Migration [18]

C. *Migration Module*

Movement module is a product part in the Virtual Machine Manager that permits real-time relocation of VM's. A visitor OS can speak with the host framework and the other way around. In addition, the host framework has full authority over the entirety of VM's running over its VMM. On the off chance that the assailant can com-guarantee the VMM by means of its relocation module, at that point the respectability of all visitor VM's that are running over this VMM will be influenced. Any VM later on that will migrate to the affected VMM will in like manner be undermined. VM with a low security level is abused using the strike systems in the migration module. Exactly when an aggressor finds a VM with a low security level in the midst of the migration technique, they will attempt to deal it and can do it viably. They can use it as a gateway to deal other VM's on a comparative host with progressively raised measures of security [18]. In addition, the assailant will most likely assault the VMM itself, in the wake of distinguishing an approach to enter the framework.

IV. Examination of existing arrangements and methodologies

In this area, we have recognized and figured basic security necessities that ought to be accommodated secure live and disconnected VM relocation in Cloud space. Following is the portrayal of every one of these prerequisites. We have likewise played out a broad investigation of existing arrangements as for these security necessities. Table II, is the aftereffect of our broad investigation as for security angles:

A. *Security Prerequisites for VM movement*

We have recognized the accompanying security prerequisites for the live VM movement process. These necessities must be joined in secure live VM relocation process [6, 7].

1. Uprightness confirmation of Stage: The objective stage cryptographically separates itself to a hotspot for trust establishment.
2. Authentication: Aggressor can dispatch MITM assault utilizing system, for example, course capturing or ARP harming in the movement procedure. So as to maintain a strategic distance from MITM assaults on live VM relocation, source and goal stages should commonly confirm one another.
3. Authorization (Access Control Policies): Proper access control arrangements must be given to verify the live VM movement process. An unapproved client/job may dispatch VM start, relocation activity. Unapproved exercises can be avoided utilizing access control list (ACL's) in hypervisor.
4. Confidentiality and Integrity of VM during migration: A mixed channel must be set up so an attacker can't get any information from VM substance and change of substance can be suitably recognized. This will keep up a key separation from dynamic attacks, for instance, memory control on live development and uninvolved strikes, for instance, spillage of tricky information.
5. Replay resistance: Assailant can catch traffic and replay it last to get validated in VM movement process. In this way live VM movement procedure ought to be replay safe. Nonce's can be utilized to anticipate replay assault in relocation.
6. Source Non-repudiation: Source can't deny from VM relocation task. This element can be accomplished by utilizing Public key Certificate.

B. *Existing VM Movement arrangements*

In confined development sort out a way to deal with source and objective VM's amassed into Virtual LAN (VLAN). It withdraws the development of traffic from other framework traffic. Disconnection of movement traffic will lessen the threat of introduction [6, 8].

Network Security Engine-Hypervisor (NSE-H) based strategy is an enlargement to Hypervisor. It has firewall, IDS/IPS functionalities for confirmation against interferences in virtual framework. Its designing involve Virtual Machine Migration Agent (VMMA), Security Context Migration Agent (SCMA), and Live Migration Coordinator (LMC) sections [6].

Technique/Role based development approach uses Intel vPro advancement for confirmation of migration process. It involves Attestation Service, Seal Storage, Policy Service, Migration Service and Secure Hypervisor parts [6, 9].

Secure VM-vTPM movement convention involve approval, confirmation and data trade stages. In the essential stage, the two social occasions normally approve each other and set up secure session for ensuing correspondence. After confirmation and secure channel establishment, remote validation performed by source to check/affirm the system trustworthiness. In the last development, VM and vTPM trade occurs. Source have first suspends the VM along vTPM, scramble them and after that trade to objective machine. Besides, source have also eradicates VM along its vTPM [6, 10].

The improved vTPM movement convention contains the establishment of trusted channel and secure data trade stages. In establishment of trusted channel arrange, first the two social affairs normally affirm each other and after that property based remote affirmation is done by source host to check/check the uprightness. The two get-togethers organize cryptographic framework, hash designs and key exchanges using DH key understanding tradition. After establishment of a confirmed and secure session, VM and vTPM trade part is begun. Source have suspends the VM and its related vTPM and takes hash of vTPM portions. Encryption on VM and the vTPM group is performed and thereafter traded to objective have [7].

Kenneth et al [11] proposed configuration involves burying cloud middle people, a protected channel between go-betweens, migration with non-shared limit and virtual framework development parts. Cover cloud delegates used to keep access to those hosts which are used in bury cloud VM transportability. The go-between server at the source and objective fogs talks with each other and covers the nuances of the source and objective Cloud has. SSH tunnel is set up between go-betweens for secure VM migration and VM states and memory is traded in the midst of the development strategy.

Trusted Cloud Security Level (TCSL) proposed new designing for cloud organize with set of game plans to change zones. TCSL is the reliable relationship of VM's and isolates trusted zones subject to security necessities of VM's in cloud. Each trusted zone in trusted cloud has a security level. VM movement in trusted in cloud is managed by Reliable Migration Module (RMM). It include Central Security Management, Cloud Security Management, Security Attributes and Waiting Queue for Migration layers [12].

RSA with SSL based Secure VM relocation process is includes three phases. In the first place, load depend on physical host then RSA with SSL tradition is used for check and encryption part similarly concerning affirmation and insurance of memory substance.

At long last, Pre-duplicate or Post-duplicate relocation methods utilized for live movement among source and goal [13].

Trusted Token (TT) based relocation approach contains set methodology, realize development procedure and survey movement fragments. Customer's procedure contains the attractive Trust Assurance Level (TAL) estimation of the target cloud arrange for VM migration.TT is a trust capability which contains TAL regard issued by Platform Trust Assurance Authority (PTTA) in perspective on gear and programming portions of stage. VM migration occurs if TAL regard in TT of objective stage is tasteful against the TAL estimation of customer development course of action. TPM-based tie key pair is used for encryption of VM [14].
Fengzhe et al [17] proposed secure VM migration in revamp VMM called VMM actualized confirmation system which offers security to frames in Virtual Machine. Verified memory pages are in like manner secured in VMM. Madhouse is used to keep up encryption keys for application in VM and Overshadow keeps up keys for guaranteed pages. It contain three rule modules: 1) migration data protection module, which is used to encode, interpret and square guaranteed methodology or pages in the midst of development errand 2) meta data the officials module, used to regulate (migration and generation) metadata (encryption keys, process identities, etc) at recipient end after development process 3) security ensure give security in the midst of live movement activity [17].

C. *Impediments of Existing Arrangements*

Isolated Migration Network: It just isolates the movement traffic from system traffic. It gets progressively mind boggling and authoritative cost expanded with populace of VM's [6, 8].

Network Security Engine-Hypervisor (NSE-H): NSE-H based methodology does not bolster any of the security prerequisites for VM relocations delineated in Table II [6].

Role based secure migration: It can't be consolidated with current passed on structure since changes are required at programming and gear levels. Live movement isn't supported in this philosophy [6, 9].

Secure VM-vTPM: Live movement isn't reinforced in vTPM based movement tradition. Keys of vTPM are moreover secured outside the TPM, along these lines slanted to spillage and unapproved alteration. The vTPM state is moreover moved, so it is an overhead and it grows the development time [6, 10].

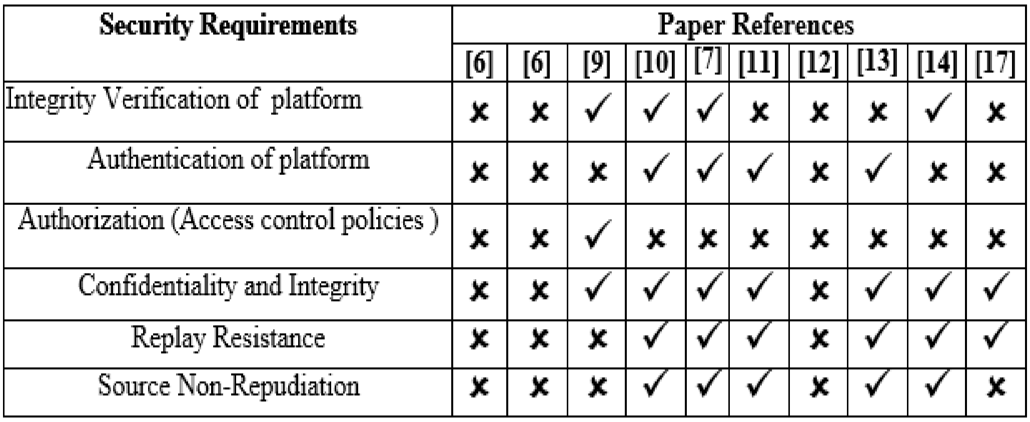
Improved vTPM migration Protocol: Live relocation isn't upheld in vTPM based movement instruments. The vTPM state is likewise moved alongside VM. It is an overhead and it builds the relocation time also [7].

VM mobility using SSH tunnel: Authorization is not supported in this solution. Furthermore it requires port forwarding on firewalls [11].

Trusted Cloud Security Level (TCSL): This procedure does not give any of the recognized security necessities for VM development. TCSL, isolates the VM relies upon their security level in trusted in zone of Cloud. TCSL based game plans can't consolidate with existing Cloud Infrastructures. It requires changes in cloud organize for reliable and security features [12].

Secure Migration using RSA with SSL Protocol: RSA based affirmation required open keys of all hypervisors for endorsement being developed procedure. It makes the main gathering of Public keys troublesome. This theory does not acclimate to security necessities as appeared to be Table II [13].

Table Ii Examination of Existing Arrangements and Methodologies



Security Requirements	Paper References									
	[6]	[6]	[9]	[10]	[7]	[11]	[12]	[13]	[14]	[17]
Integrity Verification of platform	✗	✗	✓	✓	✓	✗	✗	✗	✓	✗
Authentication of platform	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗
Authorization (Access control policies)	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Confidentiality and Integrity	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓
Replay Resistance	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓
Source Non-Repudiation	✗	✗	✗	✓	✓	✓	✗	✓	✓	✗

Trust Token based migration: It gets intricate as a different customer in the meantime perform VM development in Cloud. TAL regard is poor upon on hardware and programming fragments of stage so a little change in stage requires new TAL regard set apart by PTTA. It will in like manner degenerate execution in light of the way that TPM is essential bottleneck in this game plan. Also, it doesn't reinforce the live VM development process [14].

Protection Aegis for Live Migration of VM's (PALM): It increases the downtime by migrating metadata along VM. Furthermore it does not provide authentication/authorization security features [17].

By far most of the present responses for VM relocation are either TPM based or disregard to work with legacy hardware, or they give VM movement security issues only. The strategy of VM relocation finished using one of the security features, for instance, encryption, gives confidentiality of data anyway its security may possibly miss the mark if other security features are absent, for instance, get the opportunity to control, shared check and data uprightness. For example, nonattendance of access control may cause unapproved VM migration realizing VM to be moved to a phase under the control of an aggressor, paying little heed to whether VM was encoded in the midst of transmission [19]. The point of convergence of proposed course of action is to address the controls of existing techniques and devise a sweeping tradition for securely moving the virtual machine in an approved and affirmed strategy. Furthermore, the procedure displayed in this paper does not present gear dependence and works with legacy hardware support. After a conscious audit of writing, following security prerequisites are considered while planning our proposed arrangement:

- Shared Access control for VM Movement Procedure
- Mutual Validation of source and goal area
- Confidentiality of VM information in travel
- Integrity of VM information in travel
- Non-renouncement of movement process

The approach presented in this paper attempts to cover all the above mentioned security issues as a single comprehensive solution.

V. PROPOSED SECURE VM RELOCATION DESIGN

After as appeared in Fig. II, in the proposed design, the procedure of between cloud virtual machine movements comprises of following advances:

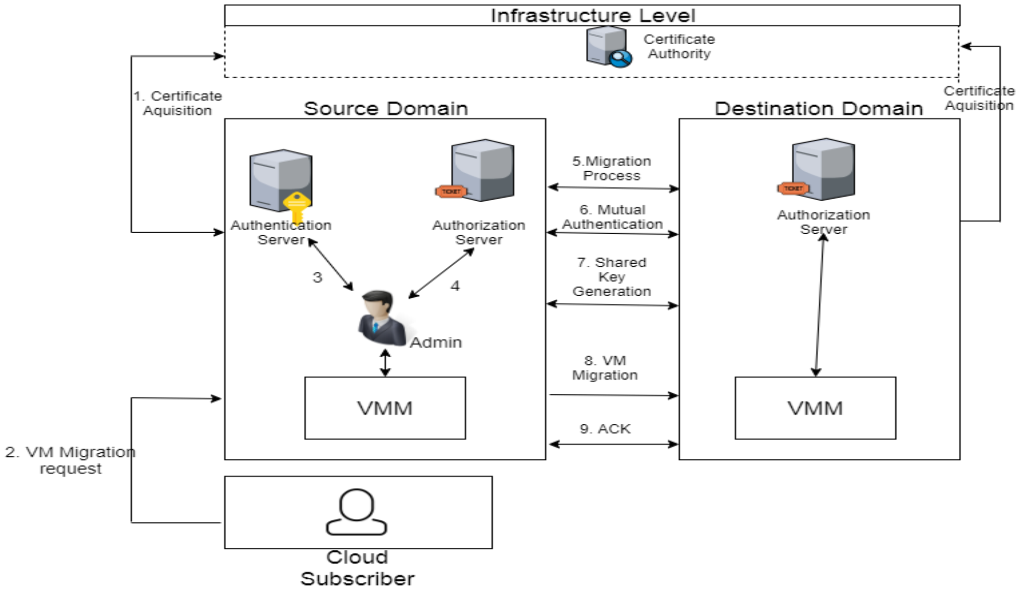


Figure 2 Proposed Architecture for Secure Live VM Migration

Step-1: Get X.509 certificates: Source and objective cloud providers are required to have X.509 certificates from a trusted Certificate Specialist.

Step-2: Demand for VM movement process commencement: The system of VM migration can be begun either by a cloud provider or by a cloud supporter. A cloud provider may require migrating virtual machine from its server homestead to another server ranch for growing its server ranch's benefits which may come up short in apex organization hours. A cloud endorser may require VM development in case he finds cost benefit with some other cloud provider.

Step-3: Verification from the nearby validation server: In the wake of affirming the accreditations shown by the migration client, the approval server gives an affirmation ticket to the development client.

Step-4: Getting approval ticket from nearby approval server: The relocation client shows the affirmation ticket to the endorsement server. After imperative verification, endorsement server issues an endorsement ticket to the migration client.

Step-5: Movement ask for to the goal cloud area: The migration client sends the development request to the objective cloud space. This request contains the open key certification of the source cloud space and the endorsement ticket issued by the endorsement server of the source cloud territory.

Step-6: Common Confirmation: The endorsement server in objective cloud space verifies the open key certificate and endorsement ticket for VM development sent by the source zone. The endorsement server in objective cloud space verifies the benefits of requesting zone for the development inquire. After needful verification, the objective space sends the positive response for the development request and moreover sends its own one of a kind open key certificate. The source cloud space verifies open key certificate of the objective cloud region. This methodology gives the common check organization to both source similarly as objective cloud spaces.

Step-7: Shared Key Generation: After the two spaces affirm each other, a symmetric expert key is made using ECDH (Elliptic Bend Diffie-Hellmann Plan) [20]. This expert key is also used to create session key to scramble the virtual machine data before movement.

Step-8: VM Information Exchange: VM data is encoded with the common key using symmetric key count for instance AES [21] and after this encoded data is sent to the objective cloud region. The trustworthiness of VM data in the midst of movement is ensured using SHA-256 hash estimation [22]. The reason behind using SHA-256 is its recommendation by the standard for the message inspect to (2)64 bits. As migratable VM data is far not as much as this size along these lines SHA-256 is sufficient consequently.

Step-9: Affirmation: Goal cloud region plays out the trustworthiness verification and after that sends back the certification message for productive trade of virtual machine data. The methodology of VM data trade and assertion continues until all the VM data is viably traded to the objective cloud territory.

VI. CONCLUSION AND FUTURE WORK

In this paper, the security essentials for secure development of virtual machine, are dismembered and it is identified that nonappearance of single security feature may rise various distinctive vulnerabilities amid the time spent VM migration. The philosophy presented in this paper gives diverse security benefits as a singular complete response for secure VM development to an approved and affirmed condition. The proposed tradition at first plays out the area check and endorsement of development client. The endorsement servers on both of the source and objective zones generally approve the spaces (using Federal Information Processing Standards-196) through exchange of cautiously checked tick. A symmetric session key is made on the two terminations using ECDH and VM data is mixed in the midst of transmission using AES. For data uprightness SHA-256 is used. Additionally, least possible cover space message exchange for shared approval of regions make the tradition secure just as efficient as well. The future work fuses the execution of the proposed building.

REFERENCES

[1] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications 2013.

[2] P. Mell, T. Grance, 'The NIST definition of cloud computing". NIST,Special Publication 800–145, Gaithersburg, MD.

[3] J. Oberheide, E. Cooke and F. Jahanian, "Empirical exploitation of live Virtual Machine migration", Proc. of BlackHat DC convention 2008.

[4] V. Vaidya, "Virtualization vulnerabilities and threats: a solution white paper", RedCannon Security Inc, 2009. http://www.redcannon.com/vDefense/VM_security_wp.pdf.

[5] Steve Orrin, Virtualization Security: Challenges and Solutions, 2010. http://365.rsaconference.com/servlet/JiveServlet/previewBody/255 5- 102-2-3214/STAR-303.pdf.

[6] J. Shetty, Anala M. R, Shobha G, "A survey on techniques of secure live migration of virtual machine", International Journal of Computer Applications (0975 – 8887), vol. 39, no.12, February 2012.

[7] X. Wan, X. Zhang, L. Chen and J. Zhu, "An improved vTPM migration protocol based trusted channel", International Conference on Systems and Informatics, 2012, pp. 871-875.

[8] OpenStack Security Guide, 2013. http://docs.openstack.org/security-guide/security-guide.pdf.

[9] W. Wang, Y. Zhang, B. Lin, X. Wu and K. Miao, "Secured and reliable VM migration in personal cloud", 2nd International Conference on Computer Engineering and Technology, 2010.

[10] B. Danev, R. J. Masti, G. O. Karame and S. Capkun,"Enabling secure VM-vTPM migration in private clouds", Proceedings of the 18th Annual Computer Security Applications Conference, December 05- 09, 2011, Orlando, Florida.

[11] K. Nagin, D. Hadas, Z. Dubitzky, A. Glikson, I. Loy, B. Rochwerger and L. Schour, "Inter-cloud mobility of virtual machines", International Conference on Systems and Storage, May 30-June 01, 2011, Haifa, Israel.

[12] Y. Chen, Q. Shen, P. Sun, Y. Li, Z. Chen and S. Qing, "Reliable migration module in trusted cloud based on security level – design and implementation", International Parallel and Distributed Processing Symposium Workshops & PhD Forum 2012.

[13] V. P. Patil and G.A. Patil, "Migrating process and virtual machine in the cloud: load balancing and security perspectives," International Journal of Advanced Computer Science and Information Technology 2012, vol. 1, pp. 11-19.

[14] M. Aslam, C. Gehrmann, M. Bjorkman "Security and trust preserving VM migrations in public clouds", International Conference on Trust, Security and Privacy in Computing and Communications 2012.

[15] P. Botero, Diego "A brief tutorial on live virtual machine migration from a security perspective", University of Princeton, USA.

[16] A. Rehman, S. Alqahtani, A. Altameem and T. Saba, "Virtual machine security challenges: case studies", International Journal of Machine Learning and Cybernetics: 1-14, April 2013.

[17] F. Zhang, Y. Huang, H. Wang, H. Chen, B. Zang, "PALM: security preserving VM live migration for systems with VMM- enforced protection", Third Asia-Pacific Trusted Infrastructure Technologies Conference, 2008.

[18] Anita Choudhary, Mahesh Chandra Govil, Girdhari Singh, Lalit K. Awasthi, Emmanuel S. Pilli, Divya Kapil, "A critical survey of live virtual machine migration techniques", Journal of Cloud Computing, Springer, November 2017

[19] Xianqin, C., et al.: Seamless virtual machine live migration on network security enhanced hypervisor. In: IEEE 2nd International Conference on Broadband Network & Multimedia Technology, (IC-BNMT), pp. 847–853. IEEE (2009)

[20] Recommendation for Pair Wise Key Establishment Schemes using Discrete Logarithm Cryptography (Revised), NIST Special Publication 800–56A (2007)

[21] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197 (2001)

[22] Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4 (2012)