DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4993

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

PARAMETRIC ANALYSIS TO ENHANCE SECURITY IN CLOUD COMPUTING TO PREVENT ATTACKS IN LIVE MIGRATION

Gurdeep Kaur
Department of Computer Engineering and Technology
Guru Nanak Dev University
Amritsar, Punjab

Sandeep Sharma
Department of Computer Engineering and Technology
Guru Nanak Dev University
Amritsar, Punjab

Abstract: Cloud computing is an emerging field of today's era to provide numerous services to the users. By using application software's like net browser, IT users will get these services dynamically over the internet. Virtualization technology can provide these kinds of services by live migration. During live migration process VMs are reallocated from one physical host to another without disconnecting the application.In the live migration technique security of the vrtual machines is a very important issue. Existing security models does not guarantee complete security of live migration process. In this paper, we tend to discuss the various security concerns, attacks on LM and solution approaches that are Network Isolation (VLAN), v-TPM LM protocol, NSE-H and The CoM Security Framework, role based migration, SPLM Model, The Live Migration Defence Framework and The Protection Aegis for Live Migration (PALM). The comparison among these solutions based on the security dimensions is also given.

Keywords: Live Migration(LM) , Virtual Machine(VM), Security, Cloud Computing.

1. INTRODUCTION

This paper presents techniques for secure live migration in cloud computing. Cloud computing is the delivery of on demand infinite computing resources over the Internet. In each trade and academe, cloud computing has attracted significant attention [16]. Cloud computing is a pay-per-use model wherever Infrastructure (IaaS), Platform (PaaS) and software (SaaS) system are often accessed as a service. Cloud computing uses the conception of virtualization and utility computing [18].

Virtualization technology was planned in the late 1960s by IBM, could be a framework or methodology are suggested for dividing the resources of a computer into varied execution environments [7]. Virtual Machine (VM) act as a guest machine on a host machine, same as a Physical Machine (PM) has united resource levels of input/output (I/O) devices, processor, and memory [19]. Hypervisors additionally called Virtual Machine Monitor (VMM) is the most significant part of virtualization that acts as a layer between the real hardware and virtualized operating system [9]. Virtualization technology permits the sharing of same physical resources among many users which helps to make utilization of resources efficiently and effectively [6]. The type 1 hypervisors are most popular over type 2 hypervisor as a result of type 1 hypervisor deal directly with the hardware and thus give higher performance efficiency, availability and security [9].

Live migration of Virtual Machines is a fundamental highlight of virtualization. Usually, migration of VM's has been done in an offline fashion. On the destination side, the Virtual Machine (VM) operations need arranging to make resumed, at a point when the migrated started with particular case server on an additional. More recently, on-line migration technology (Live Migration) has become obtainable [17]. Live migration is a process refers to the migration of a virtual machine (or entire OS and its associated applications) in a dynamic and transparent manner from one physical machine to a different whereas the virtual machine remains running. The Virtual machines are migrated lively with a minimum time period and while not interrupting the application running on the source VM [3].

A protected live relocation needs:

- Confirmed and approved administration capacities (i.e. VM creation, cancellation, relocation and so on).
- A system to identify and report suspicious exercises.
- The source and destination stages are trustworthy.
- The migration information should remain confidential and unrestricted throughout the transmission.

Generally, the live movement technique needs the standard safeguard inside and out approach for it to be secured [8].

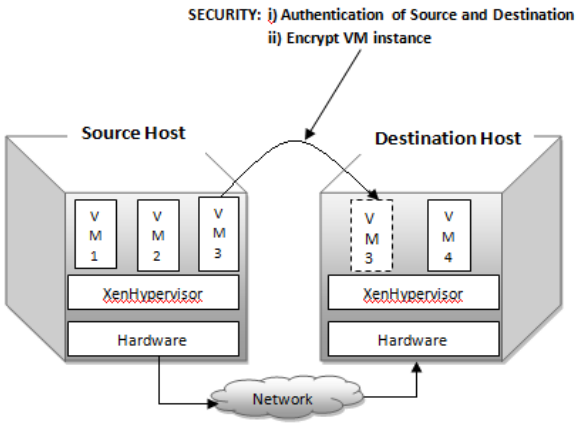


Figure1: Secure VM migration[4]

Security is a major concern in the live migration process. Attaining ability is difficult and guaranteeing consistency of

all VMs could be a basic issue. The analysis relies on the approaches for live VM migration with vulnerabilities within the relocation method. Additionally, some security methods to reduce the attacks and threats during live migration of VM's are also mentioned.

1.1 Procedure of live migration

Running Virtual machines are migrated from one physical host to another using Post-copy and Pre-Copy methods in live migration. This process involves several stages [2].

Stage 1: In the starting phase, the virtual machine to be migrated from one platform to another is chosen and after that TCP connections are established [2].

Stage 2: Memory pages of a virtual machine are shifted from source machine to destination platform in memory shifting stage[4].

Stage 3: Storage Transfer Stage

Control storage from Storage devices (such as virtual hard disks) transferred from one physical server to the destination host then destination host will be an updated virtual machine and access to any associated data-storage medium [2].

Stage 4: Network Clean-up Stage

For a clear migration, all system associations that were open before relocation should stay open after relocation finishes. Since every VM will have Virtual Network Interface card (VNIC) which is recognized by a MAC address, the VM needs to refresh the switches in the system with the goal that the virtual machine activity will be sent through the relating switch port.

[2][4]

1.2 Methods of Live Migration [12]

Pre Copy	Post Copy
To begin with exchange the memory and later exchange the execution from one host to another	To begin with exchange the execution and later exchange the memory from one host to another
Downtime is less than one second. On aborting migration, system doesn't crash because of running VM in source host	As we know downtime varies with the type of the migration technique. Downtime is more in Post Copy method as compared to Pre Copy
Overhead of duplicate page transmission	Memory transferred during a single pass and has less network overhead

This paper is prepared as follows. Section 2 describes security dimensions of live migration, subsequent section 3 includes some solutions to prevent attacks in live migration, section 4 include a comparison of various encryption algorithms, the last section consists of conclusion.

2. VARIOUS SECURITY DIMENSIONS IN CONTEXT OF LIVE MIGRATION TECHNIQUE

Requirements for Secure Live Migration are as follows:

Access Control or Authorization

- Used to control the access of particular data or information.
- Inaccurate access control strategies may enable an unapproved client to control virtual machines, for example, beginning, halting, or moving virtual machines.
- With a specific end goal to keep the virtual machine from being assaulted, the ACL (Access Control List) must be executed to anticipate unauthorized access [10].

Authenticity

- Its main purpose is to confirm the identity of the individual. In this, we determine whether or not the user has an access to an exact kind of resources and the usage authority to prevent the attacker from getting access to resources of legitimate users.
- Live relocation can be powerless against a few attacks like **Man-In-The-Middle Attack**, **Denial of-Service (DOS)** and **Stack over flow** [2]. To avoid the MITM (Man-In-The-Middle) Attack, DOS (Denial of Service) Source and Destination host must perform mutual authentication or common confirmation when the virtual machine is ready to migrate [10].

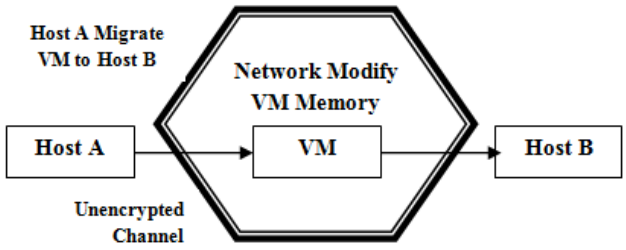


Figure2: MITM (Man-In-The-Middle) Attack launch by attacker in migration procedure using route hijacking [10]

- LM is normally started from heavily loaded VMM to a different less loaded one in Dynamic Load Balancing. In this, a malicious Virtual Machine (VM under control of attacker) might hamper the migration process. Another possible scenario is once a malicious end-consumer exploit this option by way of overloading a server and creates a huge number of VMs designated the load balancing function to migrate one or more than one VMs to a different host [13].
- In addition, System Administrator can control the migration process through the management console. Because Administrator is approved personnel with rights to perform pivotal configuration and set-ups, so it may be attacked by an attacker and the attacker will fake to be a supervisor to implement malicious migration [2].

Non-Repudiation

During the Live Migration process, there is a need to control and monitor all the activities privately by the System Administrator either automatically or manually.

Data Confidentiality & Integrity
Data is not automatically encrypted in LM, so it can be hacked by an attacker. By using Security techniques data must encrypt properly on the server side before transmission. This will help to avoid attacks during migration, such as passive attacks (leakage of sensitive data) and memory manipulation in LM [2].

Link transmission security
An Attacker can perform various attacks on an unprotected transmission channel. **Passive attacks** include sensitive information, confidential information, passwords or user account. **Active Attacks** are more serious because it directly affects the Virtual Machine, destroying the virtual machine eventually [13].
So to avoid such attacks we need to protect transmission channels for migration using SSL channel or VPN tunnel mechanism [13].

Secrecy or Privacy
In secrecy, a malicious user might migrate a malicious virtual machine to the physical server, and alternative virtual machines on the physical machine will simply be damaged by the malicious virtual machine and the corresponding user info is simple to leak [20].

3. ATTACKS ON VM AND EXISTING SOLUTIONS FOR SECURE LIVE MIGRATION TECHNIQUE

Jon Oberheide et al express the requirement for secure migration process using observations [21]. To overload goal server, an unapproved attacker will provoke large quantity of outgoing migrations onto a legitimate virtualized host server and it decreasing its performance of service. This is known as a denial of service attack [8]. The unauthorized attacker can migrate VM to authentic target hypervisor with malicious code, provides a platform for malicious VM to accomplish internet attacks on a target machine and gaining control over the hypervisor [8].

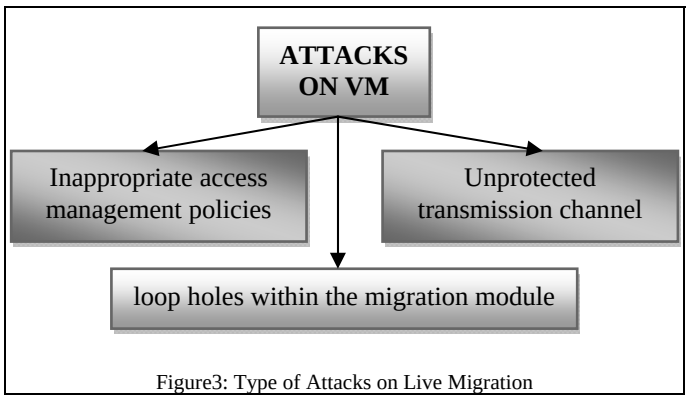


Figure3: Type of Attacks on Live Migration

Here we tend to discuss some existing solutions, which may provide a secure system.

A. VLAN - Network Isolation

In this approach, a group of VM's is formed in order to separate the migration traffic.The limitation of this method is that by increasing the VMs on network, the complexity of network and maintaining cost also grows [7].

B. An improved Virtual-Trusted Platform Module (v-TPM) LM protocol

This protocol basically makes a secure connection between the source machine and destination machine. This protocol works in following four phases:
Phase A: Authentication (Secure, trusted & private Session Establishment)
To select an encryption standard (like AES, ECC, RSA) to protect integrity and confidentiality of data, TLS (Transaction Layer Security) protocol is used for handshaking. As shown below, using RSA encryption method pre master key is exchanged and then using pre master key two keys (Key_{enc}, Key_{mac}) are generated for further encryption and integrity checking using SHA-1 [8]

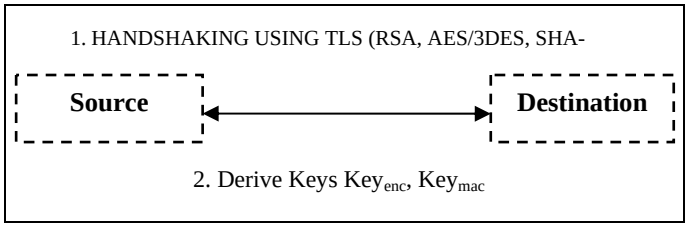


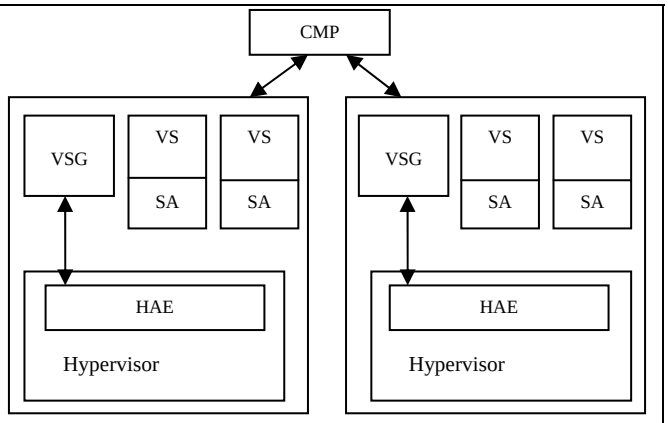
Figure4: Secure, trusted & private Session Establishment [8]

Phase B: Firstly source will create a nonce and sends attestation request to the destination machine. Then destination creates a new nonce two and sends to the source, which helps to make sure freshness of the VM-vTPM transfer within the next part. The source will send two types of messages to the destination:
a. For locking, it sends SVR_ATT_OK message.
b. In case of failure, it sends SVR_ATT_FAILED [8]
Phase C: Data transfer stage (vTPM and VM transfer)
Concatenation of vTPM corresponds to its VM is encrypted using key_{enc}. Then (Resulting message + HMACK) is computed using Key_{mac}. Then source can move this encrypted knowledge towards the destination. On successful completion of method, source platform can get acknowledgment DONE from the destination side [8].
Phase D: The last stage of this method is a deletion of the v-TPM at the source side.

C. SPLM (Security Protection of Live Migration) Model

For a large number of VMs, SPLM model is more suitable. Figure 5 shows the architecture of SPLM model. In this model, CMP (Centralized Management Platform) is for the security of centralized management by supporting the security policies. VSG protect the communication between virtual machines by getting communication data through HAE. More detail about this model given in [13] paper. At last, we say that this model is better for a large number of VMs as compare to other models [13].

SPLM model is based on encryption. Migration time in SPLM is more as compare to other traditional methods due to the encryption of migration data.



CMP: Centralized Management Platform
VSG: Virtual Security Gateway
SA: VM Security Agent
HAE: Hypervisor Access Engine

Figure5: Architecture of SPLM Model [13]

D. Network Security Engine (NSE)- Hypervisor (The CoM Security Framework):

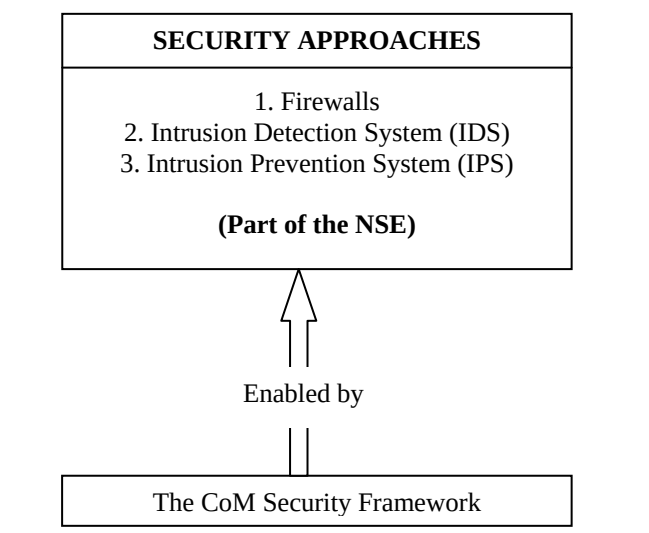
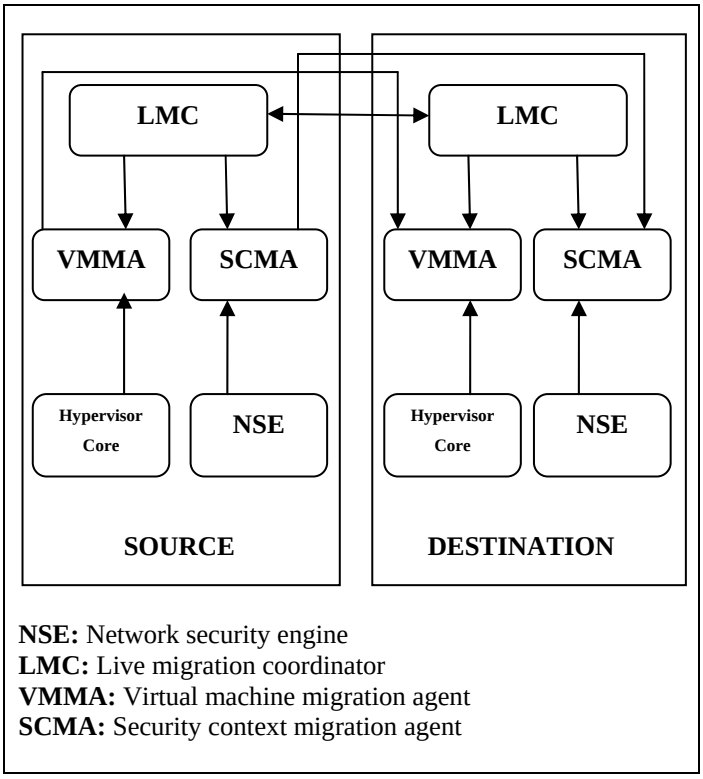


Figure6: Main Task of the CoM Security Framework[2]

In this approach, a migration information security context is transferred in order that VM is restored on target stage [7].
The NSE firewall work in state full method, NSE maintain security context (SC) for every packet and additionally construct selections supported security context (SC) and content of the packet. The problem arises at the destination, which has an effect on as a result at the destination the VM is rejected due to missing or not matching needed security context.
Figure 7 shows the architecture and components of COM framework [19].



NSE: Network security engine
LMC: Live migration coordinator
VMMA: Virtual machine migration agent
SCMA: Security context migration agent

Figure7: The CoM Architecture [8]

-VMMA is acting as an agent which interacts with the hypervisors VMMA of the target system.
-SCMA is also an agent which encapsulates and sends VM related SC set at once via a dedicated channel
-Live migration coordinator (LMC) is a coordinator which immediately works together with target system hypervisors LMC and schedules the 2 agents parallel carry out a task of migration. Preparation, Iterative Synchronization, Final Synchronization and Resumption are the four Stages of CoM architecture [19].

E. Role Based Migration:

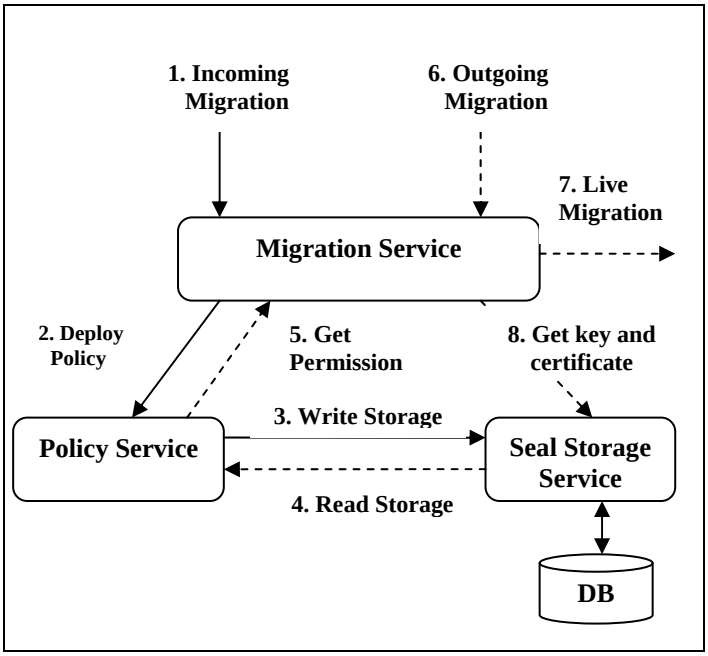


Figure8: Role Based Migration [8]

F. The Live Migration Defence Framework-(LMDF)

While considering enforcing live migration on a huge scale which includes in Cloud environment, it's far essential to keep in mind the fact that various data centers hold by cloud vendors are in distinct international areas and they do not provide particular data whether internal live migrations are used. Because of this running VMs may be live migrated without the expertise of the owners who keep their data inside these VMs. When the VMs are near the national borders while crossing then the internal data in the VM can become subject to a different legislation. Moreover, during live migration, VMs may need a manipulation in the untrustworthy area.

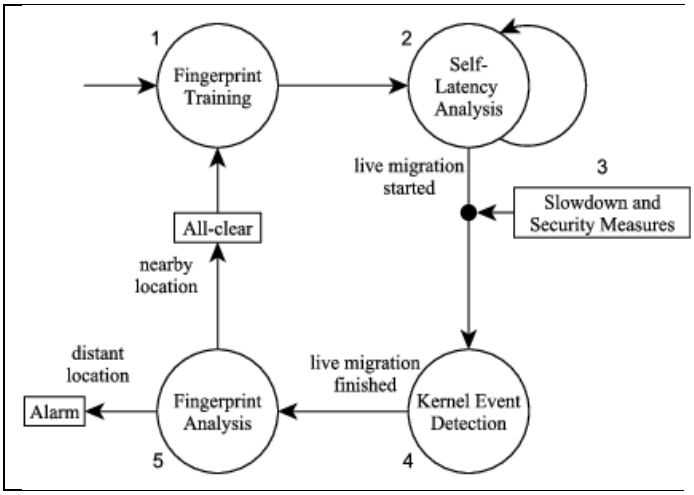


Figure9: The LMD Framework [11]

So, Live Migration Defence Framework (LMDF) has been introduced to overcome this problem of untrustworthy. It ensures the integrity and confidentiality of internal data before migration starts. The framework goals at performing as many measurements as feasible and transmits those values for later evaluation before the live migration is completed [11].

G. PALM-(The Protection Aegis for Live Migration)

PALM is depended on the VMM protection machine. In order to protect the method granularity, the VM is no longer a black-box. The VMM can have the right to understand the processes and their runtime states. Therefore the info of them is kept within the VMM, even each protected page. However, authentication and authorization security dimensions do not provide by PALM and also in this system due to the migration of metadata, the downtime is more [14].

4. COMPARISON OF LIVE MIGRATION SECURITY SOLUTIONS ON THE BASIS OF SECURITY DIMENSIONS

Two comparison tables are shown below, one is based on the comparison of some existing solutions for security in LM and in the second table we compare the various papers based on some of the main points which includes the name of the article, revealed year of the paper, models, tools, techniques, metric(s) names that's been used in the paper, the main objective and problems that paper mentioned followed by strengths and limitations that have been discovered within the paper.

Table I: Shows the comparison between the existing solutions for security in Live Migration

SECURITY -DIMENSIONS	***Network Isolation (VLAN)***	***v-TPM LM protocol***	***NSE-H and The CoM Security Framework***	***Role Based Migration***	***SPLM (Security Protection of Live Migration) Model***	***The Live Migration Defence Framework-LMDF***
Data Integrity	NO	YES	NO	YES	YES	YES
Data Confidentiality	Depends on VLAN setting	YES	NO	NO	YES	YES
Non-Repudiation	YES	YES	YES	NO	YES	NO
Link Transmission Security	NO	YES	NO	NO	YES	YES
Authenticity	Depends on VLAN setting	YES	YES	YES	YES	NO
Availability	YES	NO	YES	YES	NO	NO
Privacy	NO	YES	YES	NO	YES	YES
Authorization	Depends on VLAN setting	NO	YES	YES	YES	NO

Table II: Comparison of existing Literature Reviews

Reference of the Article	*Year*	*Models, Techniques & Tools*	*Metric (s)*	*Comments*	*Strengths*	*Limitations*
[23]	2017	- Combination of Advanced Encryption Standard (AES-256) , Information Dispersal Algorithms (IDAs), Secure Hash Algorithm (SHA-512) - Cauchy Reed Solomon (C-RS) - Windows 7 OS (Redmond,WA, USA) with 8-core Intel Xeon E5-1620 (Santa Clara, CA, USA)	• 256 bit key length(encryption key k) • size(KB) of the data • value of the (m,n)threshold, *//where m is a number of symbols/bytes required to reconstruct F'(encrypted data) and n is a total number of slices* • encoding/ decoding time(in sec)	This algorithm achieves far a greater degree of security to secure data privacy for small and large files as compared to other security approaches.	• To overcome the problem of data leakage and corruption. • Decoding process provides the highest performance for small and medium data size. • Provide faster execution time • This model ensures data confidentiality, data integrity, and data availability	• This model does not guaranty data integrity and availability • Verification time increases when we choose a small threshold value of (m,n) for encoding and decoding operation. • Reconstruction time increases when the threshold value is large enough. • Encoding and decoding processes become a computationally costly for large data size.
[13]	2016	- SPLM model	-the memory size of VM (in MB) - downtime(in ms) - migration time (in ms)	This model is best for security over all existing solutions. It is based on the security policy transfer and encryption	• Highly Secured • Ensures authentication and access control • Confidentiality and integrity of data	• Migration time increases because it takes time to encryption.
[24]	2016	- RSA, AES encryption algorithms - HMAC (Hashed Message Authentication Code)	• Execution Time • Checksum	In this, a framework is designed to provide a security	• Due to indexing, Searching is easy. • Gives better execution time by studying various cryptographic methods	• Time complexity isn't given • Algorithm is not validated mathematically
[12]	2015	- AES, 3DES encryption algorithms - QEMU/KVM hypervisor (qemu-kvm version 0.12.3 & Yabusame QEMU/KVM) - OpenSSH version 5.9 (SSH2 protocol)	• Migration Bandwidth(in MB) • Downtime(in seconds) • migration time (in seconds) • number of pages transferred • network page faults • Minor page faults	VM migration time depends on the type of encryption algorithm or On a VM applications, during migration the performance impact varies with the type of the application and the migration mechanism.	----	----
[10]	2015	- Elliptic Curve Cryptography (ECC) -XEN Hypervisor Protocol	• Downtime (in ms) • migration time of VM (in ms)	Use encryption method to secure virtual machine migration with less migration time.	• Help to reduce threats and vulnerabilities • Improved efficiency	• Downtime is more • Performance is not so great
[22]	2015	-vTPM-VM LM protocol	•	The channel becomes trustworthy by using a virtual TPM-based integrity verification policy,	• Enhance the security in vTPM-VM live migration • Channel becomes more secure and trusted • Resistant to all software kinds of normal attacks	• Key data text cannot be decrypted • Security of LM is not guaranteed if an attacker gets the administrative privileges • Security is still under threats during malicious attacks
[2]	2014	- X.805 security standard	----	Eight security threats are analyzed and on the basis of them, we see that solution of threats addressed different security dimension. And there is not a single method which ensures a full security.	• X.805 security standard helps us to get information about all models merit and demerits	• No integrated approach has been proposed to address all of the security parameters
[11]	2013	- LMDF (Live	----		• Data integrity &	• Does not ensure access

		Migration Defence Framework) -Amazon Elastic (EC2) Platform			confidentiality • Security • Use for data protection in untrustworthy area	control and authentication • No availability
[1]	2012	-PALM prototype	- migration time - downtime	Privacy, Integrity, and Protection, modules for the protection of sensitive data are designed which ensures the security strength. Due to high downtime Performance degrades	• Guarantees the security strength is not lowered during and after the migration	• Performance degradation due to high downtime

5. CONCLUSION AND FUTURE WORK

In this survey paper, we have mentioned various security parameters, attacks and also mentioned various solutions to tackle these threats. Till now plenty of research papers have been published on the security of live migration, several frameworks have been already proposed by authors to secure live migration process but no solution addressed all the security issues (like authentication, access control, security etc.) and does not ensure the whole system security. In future, this addressed problem can be extended to make an integrated solution atmosphere that addresses these security concerns of live virtual machine migration and provides an accurate secure system.

6. REFERENCES

[1] Zhang, Fengzhe, and Haibo Chen. "Security-preserving live migration of virtual machines in the cloud." Journal of network and systems management 21.4 (2013): 562-587.

[2] Aiash, Mahdi, Glenford Mapp, and Orhan Gemikonakli. "Secure live virtual machines migration: issues and solutions." Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on. IEEE, 2014.

[3] Desai, Megha R., and Hiren B. Patel. "efficient virtual machine migration In cloud computing." Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on. IEEE, 2015.

[4] Patil, Varsha P., 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 1.1 (2012): pp-11.

[5] Xianqin, Chen, et al. "Application-Transparent Live Migration for virtual machine on network security enhanced hypervisor." China communications 8.3 (2011): 32-42.

[6] Hu, Wenjin, et al. "A quantitative study of virtual machine live migration." Proceedings of the 2013 ACM cloud and autonomic computing conference. ACM, 2013.

[7] Kadam, Rajesaheb R., and Manoj Bangare. "A Survey on Security Issues and Solutions in Live Virtual Machine Migration." International Journal of Advance Foundation and Research in Computer (IJAFRC)(December, 2012). ISSN (2014): 2348-4853.

[8] Shetty, Jyoti, M. R. Anala, and G. Shobha. "A survey on techniques of secure live migration of virtual machine." International Journal of Computer Applications 39.12 (2012): 34-39.

[9] Pandya, Tanvi. "Live Migration in cloud and its security concerns: A survey." (2015).

[10] Divyambika, R., and A. Umamakeswari. "Protection of virtual machines during live migration in cloud environment." Indian Journal of Science and Technology 8.S9 (2015): 333-339.

[11] Biedermann, Sebastian, Martin Zittel, and Stefan Katzenbeisser. "Improving security of virtual machines during live migrations." Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. IEEE, 2013.

[12] Hu, Yaohui, et al. "Performance analysis of encryption in securing the live migration of virtual machines." Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on. IEEE, 2015.

[13] Sun, Degang, et al. "SPLM: security protection of live virtual machine migration in cloud computing." Proceedings of the 4th ACM International Workshop on Security in Cloud Computing. ACM, 2016.

[14] Zhang, Fengzhe, et al. "PALM: security preserving VM live migration for systems with VMM-enforced protection." Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific. IEEE, 2008.

[15] Aiash, Mahdi, Glenford Mapp, and Orhan Gemikonakli. "Secure live virtual machines migration: issues and solutions." Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on. IEEE, 2014.

[16] Zheng, Jie, et al. "Pacer: A progress management system for live virtual machine migration in cloud computing." IEEE transactions on network and service management 10.4 (2013): 369-382.

[17] Sun, Gang, et al. "A new technique for efficient live migration of multiple virtual machines." Future Generation Computer Systems 55 (2016): 74-86.

[18] Leelipushpam, P. Getzi Jeba, and J. Sharmila. "Live VM migration techniques in cloud environment—a survey." Information & Communication Technologies (ICT), 2013 IEEE Conference on. IEEE, 2013.

[19] Upadhyay, Ankit, and Prashant Lakkadwala. "Secure live migration of VM's in Cloud Computing: A survey." Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on. IEEE, 2014.

[20] Ristenpart, Thomas, et al. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[21] Oberheide, Jon, Evan Cooke, and Farnam Jahanian. "Empirical exploitation of live virtual machine migration." Proc. of BlackHat DC convention. 2008.

[22] Fan, Peiru, et al. "An improved vTPM-VM live migration protocol." Wuhan University Journal of Natural Sciences 20.6 (2015): 512-520.

[23] Ngnie Sighom, Jean Raphael, Pin Zhang, and Lin You. "Security Enhancement for Data Migration in the Cloud." Future Internet 9.3 (2017): 23.

[24] Bhandari, Akshita, Ashutosh Gupta, and Debasis Das. "A framework for data security and storage in Cloud Computing." Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on. IEEE, 2016.