International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A Survey on cloud migration: Frameworks and security issues

Ridhvesh R. Shethwala 1, Miren Karamta 2 and Madhukar B. Potdar PhD 3

Abstract

As the demands for resources are increasing it need to use proper technology and maximize the use of hardware and software resources. As more companies are using virtual machine rather classical infrastructure so there will be more chances of attack on it. During the large amount of workloads on the servers it need better fault tolerance and load balancing schemas. Due to heavy use of server there will be chance of DoS attack on the server. And server can't reply to legitimate user and it will reduce the all over performance of the system. So making it more reliable and secure virtual machine needs migration. During Virtual machine migration on the network, the VMs are prone to both active and passive attack. To avoid this issue, it is vital to secure the migration process. We have surveyed and analyzed the existing migration processes, their types and phases. In addition to this, we also have analyzed the existing solutions and their limitations. In this paper, we have listed and discussed security issues during migration.

Introduction to Cloud Computing

According to National Institute of Standards and Technology (NIST)" Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [4] As the demand of resources are increasing dramatically people are starting moving to the cloud services.

To use this cloud there are mainly three services are available Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Services (IaaS). In SaaS all the hardware and software is configure in the data center people just need to use those software from their web browser. [2] In PaaS cloud services provider will provide platform as service. One of the platform for developing application is install on cloud and people can direct access those platform no need for installing those platform in physical system. This will help to reduce the licenses cost of application and provide more benefits of cloud. In IaaS cloud provider will provide virtual machine to use. All the hardware resources like storage, memory, CPU, network is configure in the data center and people just need to use that machine. This will help to maximize the use of hardware resources as client side it will save cost of infrastructure.

For any small or medium scale business it need basic resources like storage space, data Center, cooling arrangement, CPU, networking components, IT support and electricity. This all will cost a lot to install and manage to reduce this cost of this, company can use the cloud service for all the thing. This services are easy to configure and managed and it will cost according to use. For license software to purchase it will cost much so cloud will provide those software as service and pay as use. The one who provide all this cloud services it called as Cloud Service Provider (CSP).

As cloud is popular more people are migrating to the cloud and it will create more challenge to adapt this technology. There are mainly two type of migrating happen as local system to cloud and one cloud service provider to another cloud service provider. People are migrating their platform like.NET from local system to the cloud as it will provide more benefits of cloud. This will reduce the license cost of company and now more people can simultaneously work on the same project and also provide mobility and full availability.

Using infrastructure as a service it will allow to maximize the use of hardware resources and can create multiple Virtual Machines using Hypervisor. [1] Hypervisor is the software that allow to maximize the use of hardware resources and let multiple operating system install and run on it. In certain situation like disaster, fault tolerance, load balancing, virtual machine need to migrate from one host to another or one service provider to another service provider.

To perform VM migrating there are mainly to approaches use pre-copy and post-copy. In pre-copy it will main machine first and then other memory content. And in post-copy it will copy memory content first and then main machine. During this migration process it need better security to prevent from different kind of attacks. To secure VM migration it need to understand the security requirements while migration. According to security requirement it need to create framework for performing

ISSN:2319-7900

secure live VM migration. In this paper we have perform survey on Migration process, security requirement during migration and available frameworks for securing live VM migration [1].

Cloud Migration

Cloud migration is the process of moving services from local environment to the cloud environment or moving from one cloud to another cloud. For Infrastructure it has Virtual machine for services. While operating VM there are some issue that occur like fault tolerance, load balancing, availability issue, reliability and more. To overcome from this kind of issue it need migration. That migration could be from one host to another host with same service provider or one cloud provider to another. This is one of the most important service as cloud adoption ratio is increasing.

A. Motivation behind Migration

Broader reach:-As we are migrating from local to cloud environment people are accessible to use the elastic nature of cloud. In cloud there is no limitation of hardware resources and computing power.

Easier mobile access:-Cloud is platform and device independent. It can be accessible form any device any operating system from any place. People can access their services from home office or from any other places.

Business agility and flexibility:-If some company want to extend service for some pick hour they are able to use as cloud has agility and as company wants to expand their services and uses they can manage more as cloud is flexible.

Improved security:-If customer is using public cloud and want more security it can move to private cloud as it has better security than public cloud. Customer can also take backup of their personal data and let them secure on cloud.

Improved responsiveness:-As cloud is independent of hardware and software installation people don't need to install any of them. People can use the services as they required. In any computation task it will be quick as many cloud system is working on it. So we can say that cloud is more responsive.

Better analytics on application usage:-cloud is pooled of resources and it will respond from that pool. For any analytics application it need more computation power, storage and ram so if people using cloud for this work it will more effective and fast.

Improved availability:-Cloud services are available for 24/7 and for 365 days and it is managed by csp. Availability is differ according to Different csp and SLA with csp. But nowadays services are so reliable and it will working on zero downtime.

Reduced and/or reallocated costs:-As people use cloud infrastructure their hardware installation cost is reduce and it will also managed by csp. For platform use it will reduce the software licenses cost. For software as services people don't need to install the software on the system and can easily use those services.

B. Types of cloud Migration [5] [6]

Replacement:-This type of cloud migration involves replacing one or more components to cloud. People are not preferring this type cloud migration as it required to reconfigure the changes from one place to another. As two different cloud provider has different architecture so it need to adjust those services. Using Amazon web services for virtual machine in place of local system is an example.

Partial:-In partial migration its process of migrate some application functionality to the cloud. For performing a particular task it will depend on one or more application layer in architecture of cloud. If people are using two different cloud services for performing one task. Using a combination of google app engine and google mail for developing application it required email services is an example of partial migration.

Whole stack:-This is the actual example of cloud migration. In this type of cloud migration it will migrate the whole stack of application from one cloud service provider to another. As we can migrating the whole encapsulated VM to another and start it on other CSP so it's not requires and type of reconfiguration. People are preferring this type of cloud migration when they need more compatible infrastructure for their work. Using amazon web services EC2 instead of OpenStack is an example of this.

Cloudify:-Cloudify means the fill cloud adaption. In this type of migration all the function of application is adopting cloud. Using infrastructure of cloud, platform application and software form cloud for developing any application is an example of cloudify.in this type of migration we are trying to make cloud-native systems.

ISSN:2319-7900

C. Phase of Cloud Migration

To performing cloud migration we need to follow certain steps to archive perfect migration. There are different phases are there for making migration more effective.

Feasibility study:-Before planning for cloud migration it need to perform feasibility study. In this part company will try to identify that migration is financially and technically feasible or not. They need to analysis the existing system for that they need to collect data of working system and try to understand the behavior of system. Company need to analysis the cost of migration according to their requirements so that they can find that migration is feasible or not.

Requirement analysis & Planning:-In requirement analysis Part Company need to identify what they need to migrate and other requirements for that. In planning phase it need detailed study of existing environment and component that need to migrate. Once study is complete then it need to know the total cost of migration.

Scheduling:-In scheduling phase it need to identify the time when migration can possible. For that it need to understand the whole day process of company and chose the best time when process of work is minimum that it will less affect people and system. So once time is identified then it can be scheduled on that time.

Migration Execution: -This is the part where actual migration is performing. It is depending on which approach chose for migration.in this part actual data is transmitted and pass from one to another.

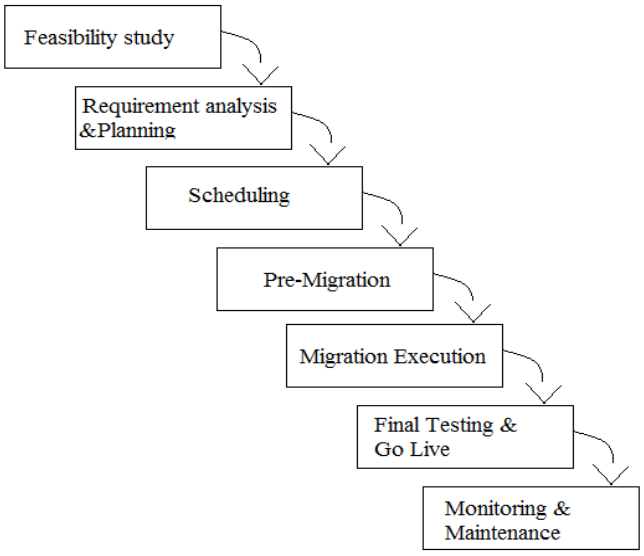

Figure 1. Phase of Cloud Migration

Final Testing & Go Live: -Before system will start it need final testing as it migrate properly or not. If its data then it need to check its checksum for integrity that all data is correctly migrated or not. Same for virtual machine migration it need to cross verification about data that transmitted. Once all is tested and data are as it is so now it is able to go live.

Pre-Migration:- This is the phase where simulation of migration is being performed and try to test the system that it is ready for migration or not. It will also help to understand the behavior of system during migration it something is not going correct then it can be changed before actual migration.

Monitoring & Maintenance:-Monitoring is important part after migrating any system. Once we migrate the virtual machine and its working correctly but still it need monitoring that it will not performing anonymously.

D. Approach of Migration

Non-live migration:-This is the simple and old technique to perform migration. As name suggested this migration in not live as the migration time period VM is not working. In the non-live migration process VM is suspended before and after the migration process. During the migration process Memory, I/O devices, state of CPU register and disk is moving to destination host. Once all the content from source is moved to destination host then it will be resumed at destination host [10]. But the problem with this approach is it takes too higher downtime.

Pre-copy Live Migration:-In pre-copy migration memory content are first copy to the destination machine but VM is still running on the source machine. As VM is still running so memory changes are there those changes called as dirty pages. As dirty pages are generate it will transmitted to the destination machine till threshold or remaining pages become less. After that VM is suspended at source machine and coping to the destination [10]. Once all the content from source is copied to destination source VM is destroyed. In pre-copy downtime is less but all over it will take more time as dirty pages are coping to destination machine [7].

Partial Live Migration:-in this type of migration only VM image is copied to the destination host. And rest of part is still at the source host. If any request come for memory access it will generate page fault. According to the need of memory on destination side source will send those memory. As this type of migration is useful when VM need to migrate for small amount of time and after some time it will be resumed to the source. This type of migration are generally

used when it need to maintain of service the server of any physical system. This type of approach is preferred when your system will be idle of long time.

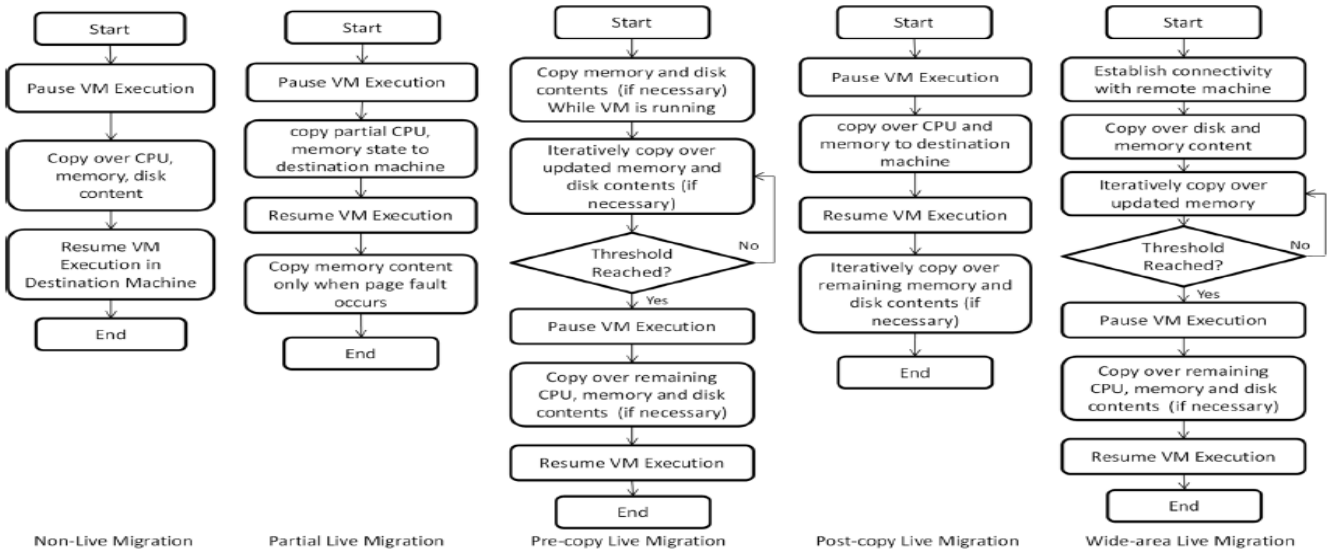

Figure 2. Different Approaches of Migration [7]

Post-copy Live Migration:-In this migration approach first it will pause the VM machine at source and copy all the current state of CPU register, disk and non-page able memory to the destination machine and then resume the VM at the destination machine. Now people are not able to access VM from destination machine. But the problem with this is someone is requesting memory which is not yet copies from source to destination. Then it will generate page fault. This page fault are redirected to the source page to resolve it. In post copy single page is transmitted in network only one when in pre-copy it will transmitted multiple time as dirty pages are occurred [10]. Pre-copy contain the latest state of the VM where in post-copy it need to wait for memory. Failure of migration in post-copy leads to loss of VM state. To reduce the page fault post-copy use pre-paging method that make priority to memory that is most important and coping them first [7].

Wide-area Live Migration:-In wide area migration its main goal is to perform migration remotely. For that it need to establish the connectivity with the remote host. Rest of it process is same as the pre-copy migration [7].

E. Performance matrix of Migration

To identify migration performance it need to consider certain performance matrix like [16]:

1). Preparation time: Preparation time is called as time taken between once it decide to perform the VM migration to it starts transferring memory from source to destination.

2). Downtime: The time when actual migration happen where source transferring its VM to destination and in between that time VM is suspended.

3). Page transferred: For any approach time taken to transfer all the memory page from source to destination.

4). Total Migration time: The time taken by the whole process from preparing for migration to the VM resume to destination and all the memory is transferred that time is called as Total Migration time.

5). Application Degradation: While performing Migration there will be chance of degradation in performance of application running on VM.

Security Issue in Different Cloud Services Migration

A. Migration in SaaS

While migrating to the SaaS service there are some threats that can occurs. If someone is changing their business model there will be some issue about loss of their control over

ISSN:2319-7900

cloud infrastructure. While using cloud service it need browser to access. If that browser it vulnerable to attacks and not provide better connection to cloud service then people will not like to migrate those services to cloud. For that it need better authentication mechanism, Secure APIs, encryption [3].

There are many attacks can be possible on SaaS migration. If the migration link is not properly secure then active and passive attacks can be possible. For that it need better encryption and hashing. Phishing attacks will also affect lot on data as people get spam mail and then they migrate their service to some fake cloud provider then their data will be lost. If the URL is not proper configured then cross site scripting can be possible and can perform Dos and buffer overflow attack [3].

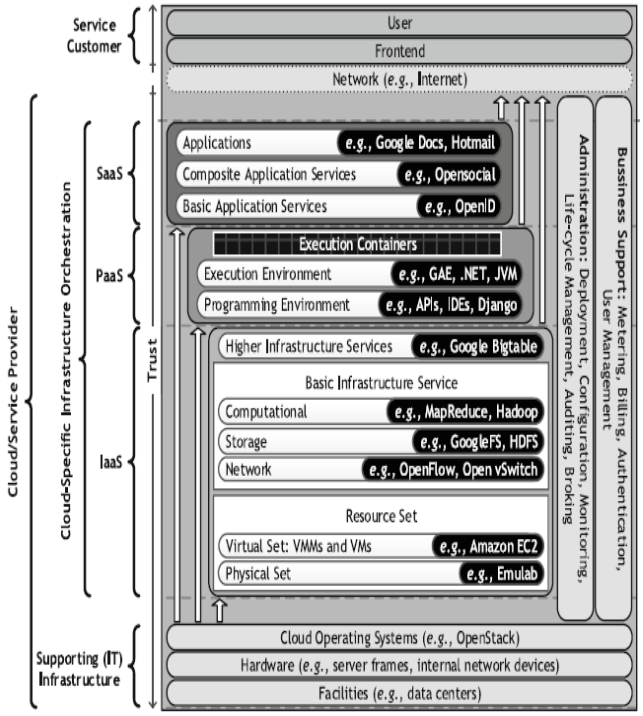

Figure 3. Different Cloud Services [1]

B. Migration in PaaS

There are many threat can be possible while migration to the PaaS. While people are migrating to PaaS their recent IDEs may need to reconfigure to the cloud so changing the business model will create some issue. If authentication system is not stronger then outsider can abuse the system and can theft our personal data and projects. While migration if it is not properly configured then there will be chances of data leakages or data losses [3].

There are some attacks possible while migrating to PaaS. If attacker send malicious link to the user and user follow that link to migrate that PaaS then their data will be lost or theft. So it need to prevent from the phishing attack. While migrating platform through any browser there will be chance of man-in-the-middle attack and attacker can take advantages of vulnerability in server or browser. In metadata spoofing attack attacker try to spoof the metadata of your application and will try to redirect you to wrong way [3].

C. Migration in IaaS

The main goal of IaaS is to maximize the use of hardware. In IaaS cloud provider will provide Virtual machine to customer as their requirement. For any small or large scale company IT infrastructure is most important and costly too. To reduce that hardware cost IaaS will be used as better alternative. Company don't need to invest in infrastructure rather using cloud infrastructure as use benefits of it. This is the best cloud service for use. As all the things are on the cloud there will be no need of physical hardware, software to install.

There are many companies are there who will provide IaaS like GoGride, Google, Amazon, VMWare, Rackspace. The main component of IaaS is the Virtual Machine. In virtual machine cloud provider will provide space, processor, ram and graphics. Combination of this resources will create a virtual machine in that data center and people can access those machine from any device using compatible browser. Customer need to pay as per they uses resources so it reduce the total cost [2].

Once any Virtual machine is created due to some issue like resource management, load balancing, expanding the service, server failure, fault tolerance, availability and some security issue Virtual Machine need to migrate. As discuss earlier there are mainly two types of migration is there one from local machine to cloud and another is one cloud VM to another cloud. And there are mainly two types of migration happen non-live migration and live migration. In non-live migration the downtime is more and it affect the availability of services so now people are moving to live migration.

Live VM migration:-In VM migration there will be two type of migration can happen one can be inter cloud provider like migrating VM from one VMWare host to another VMWare host. In second type migrating VM from One

ISSN:2319-7900

cloud provider to another like Amazon to VMWare. This two different type of migrating have different pros and cons. As in inter cloud migration cloud provider is same so it more reliable and fast. But in different cloud provider there are some issue like their Architecture, policies, security, rates, availability and Service level Agreement (SLA).

There are some threats can happen in IaaS like if customer change their business model from one cloud provider to another then there will be chance of loss of control. Its cloud provider responsibility to provide better authentication and authorization other vise services will be abused and any malicious insider or outside and attack on the system. As many customers are sharing the same hardware resources if one of the virtual machine is compromised then there will be chance of losing control on other virtual machines, so shared technology will also create issue here [3].

There are some attacks possible on the IaaS like DoS/DDoS in this type of attack attacker try to compromise one of the VM and us that to compromise other VM, attacker can use zombie system to perform DoS attack on the VM and make system down. Attacker can take advantages of shared technologies as many VM share the same hardware can perform service injection attack, VM Escape attack and attacks on hypervisor. [3]

While migrating from source to destination it need better communication channel and SSL need to be configure properly otherwise attacker can perform man-in-the-middle attack. If attacker is successful to spoof the metadata then there will be possibility of abnormal behavior of system. If attacker id performing phishing attack and generate fraud link for migration and customer use that link to migration then there will be chance of loss of data and loss of control. If attacker is successful to install backdoor in system then attacker can abuse the service later.

To prevent from this types of attack it need to follow certain steps:-

1). Try to identify the weakest link in the system and try to harden it.
2). Use properly configured SSL connection to prevent form man-in-the-middle attack.
3). Use proper authentication and authorization mechanism from preventing unauthorized use.
4). Isolation between VM's is most important as different VM are sharing the same hardware resources. And also need to properly secure the Hypervisor.

To prevent IaaS from the different attack there are some commercial solutions are available they are trying to harden the security of IaaS. Before migrating to the any cloud service provider people need to review the security products and tools offered by company and also need to understand their policy and SLA.

Literature Survey

A. Security Requirements during Virtual Machine migration

There are certain security need are there which should be fill by available approaches like [8] [9]:-

Access Control:-While migration it need access control policies that will help to reduce attack factor. Access control is required otherwise unauthorized person can perform the migration and it lead to loss.

Authentication:-Authentication is required during cloud migration otherwise malicious host will initiate the migration and it lead to loss of VM. For authentication two hosts need to establish the trust between them.

Non-Repudiation:-Migration process need to monitoring and accounting properly otherwise there will be chance of repudiation from destination host.

Data Confidentiality:-VM's data that is moving from one host to another it need better encryption standard to provide data confidentiality.

Communication security:-Communication links between two host need to be secure as providing trust channel between hosts and encryption. If links are not properly configured then there will be chance of active and passive attack.

Data Integrity:-To verify that data at destination is same as source data it need hashing to data and will provide data integrity.

Availability:-VM need to available at either side while migration. DoS attack can be possible on VM that will affect the availability of VM during migration.

Privacy:-There are some important files are there in VM. If any attack happen on VM so there will be chance of loss of those confidential files.

B. Approaches for secure VM migration

There are many approaches are there who will try to fulfil certain security requirements. But there are still some security issues are there [8] [9].

Isolate Migration network VLAN:-In this approach it will try to isolate the migration traffic from the regular network traffic to provide security during live VM migration [8]. For that it will create virtual LAN in the network and pass all the migration traffic through that. From doing this it will secure migration transmission secure as it isolate from the regular traffic and secure from many attacks [14]. The drawback of this approach is that it will only differentiate migration traffic from the network traffic this will create overhead to administrative cost. It also create complexity for configuration, maintaining virtual machines, managing growth and troubleshooting. [11].

Network Security Engine-Hypervisor (NSE-H) and CoM framework:-In this approach it will try to extend the hypervisor by adding IDS/IPS, firewall for protecting against attacks in virtual network [8] [9]. It also consists of Security Context Migration Agent (SCMA) will create dedicated channel then encapsulate all the VM security data and then send it. Network Security Engine (NSE) has state-full firewall it will provide intelligent packet filtering. Virtual Machine Migration Agent (VMMA) perform the transmission of encapsulated VM to the destination hypervisor via dedicated channel. Live Migration Coordinator (LMC) help to perform the parallel migration task with collaboration of another hypervisor [16]. The drawback of this approach is that it don't fulfill any security requirements [11].

Role Based Migration:-In this approach it use Intel Vpro technology and TPM hardware. It will provide the seal storage to secure OS and private keys. In this service it will work on role based policies and storing private keys using this private keys it will encrypt the data for trusting OS. In migration services it will first send request to remote system to check whether it reach to certain security requirements. For attention process it contain attention services which help to cryptographically identify remote hypervisor. In policy services module it will manage the all role based polices. In secure hypervisor it will provide runtime management for guest OS [11] [21]. The drawback of this approach is that it don't compatible with current Infrastructure and it don't support Live Virtual machine migration.

Secure VM-TPM:-In this approach first it will authenticate two parties by vTPM key hierarchy and established the secure communication channel. Then it will verify the remote system using hash MAC for providing integrity. Once it complete then it will encrypt the whole memory and transfer the VM [13] [20]. As it will fulfill most of the security requirements but it don't support the Live VM migration.

Improved Secure VM-TPM:-To overcome some limitation of VM-TPM approach this approach comes in the picture [8]. In this approach it will established the trusted communication channel and secure transfer of data. Once both parties are authenticated each other than secure communication channel established. And then it will verify the integrity of system and exchange the hash and key using DH key. Once all done then it will encrypt all data and transfer from source to destination [12]. This approach will fulfill many security requirement but like VM-TPM approach this don't support Live VM migration.

VM mobility using SSH tunnel:-In this technique it consists inter cloud proxies, using this proxies it will migrate. First it will get two proxy for both source and destination and then it will to make SSH tunnel between those two proxies. This will help to hide original IP of source and destination [16]. The drawback of this approach is that it required port forwarding on firewall and not supporting authorization [8].

Trusted Cloud Security Level (TCSL):- In this approach it contains policies for customize zones. It contains the logical set of VM's and isolate them according to its security requirements [8]. Each trusted zone has different level of security and managed by Reliable Migration Module (RMM). It also provide Cloud Security management, waiting queues, Central security management and security attributes [16] [19]. The drawback of the system is that it don't provide any security requirement and can't fit with existing cloud system.

RSA with SSL:-In this approach it will first perform the load balancing on source host and then perform authentication and encryption suing RSA and SSL [8]. Then it can perform any approach like post or pre copy [16] [17]. The limitation of this approach is that it will create difficulty for managing public key for all hypervisor.

Trusted Token Based Migration:-The main goal of this approach is to create trust between hosts. It contain imple-

mented migration policy, set policies and audit migration components [8]. Once trust is established between two host then it will use TPM-based for encryption [21] [22]. The limitation of this approach is that when many user want trust then it will be complex for it. As it use TPM so it contain many loopholes and it don't support Live VM migration.

Parallel Array of Linux Machines (PALM):- This approach is also called as VMM enforced protection system. For encryption key it uses CHAOS [8]. It has three module as for live migration security it's security guard will provide security, it also provide security to the Meta data as process Identification and key management, also provide encryption and decryption during migration [18]. It don't provide authorization and authentication and also it create overhead to CPU.

Security Requirements	Isolate migration network VLAN	NSEH	Role based Migration	Secure VM-vTPM	Improved vTMP based Migration	VM mobility using SSH tunnel	TCSL	Secure Migration using RSA with SSL	Trust Token Based migration	PALM	The CoM Frame work	The LMDF
Integrity Verification of platform	×	×	✓	✓	✓	×	×	×	✓	×	×	✓
Authentication of platform	×	×	×	✓	✓	✓	×	✓	×	×	✓	×
Authorization (Access control policies)	×	×	✓	×	×	×	×	×	×	×	✓	×
Confidentiality and Integrity	×	×	✓	✓	✓	✓	×	✓	✓	✓	×	✓
Replay Resistance	×	×	×	✓	✓	✓	×	✓	✓	✓	✓	✓
Source Non-Repudiation	×	×	×	✓	✓	✓	×	✓	✓	×	✓	×

Figure 4. Comparison of different approaches

The Live Migration Defense Framework (LMDF):- As all the data center are placed at different geographical location there will be chance of data loss and then it will against some policies [9]. To overcome this type of problem in this approach it detect the migration and slow down it for providing the integrity and confidentiality to it. The main goal of this approach is that it will prevent it before rather than after threat occur [15]. There will be no access control policies and it can't detect any attacks.

Summary

All the three cloud services has different way of working so they need different kind of security. In SaaS end-user don't know anything about backend infrastructure like operating system, type of server and other components used by service provider. User can only use that services from their browser and its platform independent. So most of the attacks on this type of services are browser based attacks. So reduce the risk factor of this type of attack browser needs to enhance their security and aware about latest vulnerabilities. In PaaS end-user only manage the application and data and rest of the infrastructure will be manage by the service provider. So here it need application and data security. In IaaS end-user can managed Application, data, middleware and OS and rest of hardware infrastructure will be managed by service provider. So here it need more security as more components are there to manage by the end-user. Many attacks are possible on OS, hypervisor, virtual machine.

In Virtual machine migration when it migrate from one host to another host then it need to pass through the network. As network is open to another user there will be chance of both active and passive attack on the VM. In passive attack attacker can capture the traffic passing through the network as there will be no such encryption of VM and its data. So there will be chance of breaching privacy. In active attack attacker try to perform Man-in-the-middle attack and your

VM is migrated to some different host rather selected one. So connecting link between two hosts are not safe. There are many frameworks are there for provide security during that link but somehow they can't reach to certain requirements.

This type of security framework or tools need to enhance or adapt new solution to improve the security during the migration. In future we will study more on existing solution available for securing cloud migration. And try to enhance them by creating hybrid solution or new approach.

Acknowledgment

We are thankful to Director, BISAG for providing infrastructure and encouragements.

ISSN:2319-7900

References

[1] Fernandes, Diogo AB, et al. "Security issues in cloud environments: a survey." *International Journal of Information Security* 13.2 (2014): 113-170.

[2] Chhabra, Shruti, and Veer Sain Dixit. "Cloud computing: State of the art and security issues." *ACM SIGSOFT Software Engineering Notes* 40.2 (2015): 1-11.

[3] Modi, Chirag, et al. "A survey on security issues and solutions at different layers of Cloud computing." *The Journal of Supercomputing* 63.2 (2013): 561-592.

[4] Grance, T., R. Patt-Corner, and J. B. Voas. "Cloud Computing Synopsis and Recommendations." *NIST Special Publication* (2012): 800-146.

[5] Andrikopoulos, Vasilios, et al. "How to adapt applications for the Cloud environment." *Computing* 95.6 (2013): 493-535.

[6] Rai, Rashmi, Gadadhar Sahoo, and Shabana Mehfuz. "Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration." *SpringerPlus* 4.1 (2015): 1.

[7] Boutaba, Raouf, Qi Zhang, and Mohamed Faten Zhani. "Virtual machine migration in cloud computing environments: Benefits, challenges, and approaches." *Communication Infrastructures for Cloud Computing. H. Mouftah and B. Kantarci (Eds.). IGI-Global, USA* (2013): 383-408.

[8] Ahmad, Naveed, Ayesha Kanwal, and Muhammad Awais Shibli. "Survey on secure live virtual machine (VM) migration in Cloud." *Information Assurance (NCIA), 2013 2nd National Conference on*. IEEE.

[9] 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.

[10] Ahmad, Raja Wasim, et al. "Virtual machine migration in cloud data centers: a review, taxonomy, and open research issues." *The Journal of Supercomputing* 71.7 (2015): 2473-2515.

[11] 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.

[12] Wan, Xin, et al. "An improved vTPM migration protocol based trusted channel." *Systems and Informatics (ICSAI), 2012 International Conference on*. IEEE, 2012.

[13] Danev, Boris, et al. "Enabling secure VM-vTPM migration in private clouds." *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 2011.

[14] Nagin, Kenneth, et al. "Inter-cloud mobility of virtual machines." *Proceedings of the 4th Annual International Conference on Systems and Storage*. ACM, 2011.

[15] 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.

[16] Alshahrani, Hani, et al. "Live Migration of Virtual Machine in Cloud: Survey of Issues and Solutions." *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016.

[17] 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.

[18] 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

[19] Chen, Ying, et al. "Reliable migration module in trusted cloud based on security level-design and implementation." *Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International*. IEEE, 2012.

[20] Liang, Xinlong, Rui Jiang, and Huafeng Kong. "Secure and reliable VM-vTPM migration in private cloud." *Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on*. IEEE, 2013.

[21] Wang, Wei, et al. "Secured and reliable vm migration in personal cloud." *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*. Vol. 1. IEEE, 2010.

[22] Aslam, Mudassar, Christian Gehrmann, and Mats Björkman. "Security and trust preserving VM migrations in public clouds." *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2012.

Biographies

RIDHVESH R. SHETHWALA received the B.E degree in Computer Engineering from Gujarat Technological University, Gujarat in 2011. Currently, he is pursuing his master's degree from Nirma University, Ahmedabad,

ISSN:2319-7900

Gujarat and doing his internship for final year dissertation at BISAG, Gandhinagar, Gujarat.

MIREN KARAMTA received M.tech degree in Computer Engineering from Dharmsinh Desai Institute of Technology (DDIT) in 2010. He has More than 6 years of system and network administration experience. He is very enthusiast about Open source technologies. Currently, He is working as IT Infrastructure system manager at BISAG.

DR. M.B. POTDAR is a 1982 Ph. D. in Physics from Physical Research Laboratory of Dept. of Space, Govt. of India. Later for 28 years, he was associated with the Indian Space Research Organization (ISRO of Dept. of Space, Govt. of India) in various capacities. He worked extensively in development of land and atmospheric applications of Remote Sensing data. Since March 2011, he is holding position as Project Director at BISAG and organizing and steering research in various area of software development and applications of geo-spatial data.