A Study on Cloud Migration Models and Security Issues in Cloud Migration

[1]Tulasi Vemu, [2] P. Sravya

[1,] Department of Computer Science and Engineering, GVPCE (A), Visakhapatnam.
[2]P.hD Scholar from JNTU Kakinada

Abstract: Cloud migration is the process of transferring the data, applications, operating systems and all other IT resources to cloud or a physical server. Cloud migration can also defined as migration of organizational infrastructure, computing resources, physical storage, Operating Systems, platform services and software are moved to the cloud. It is often involves combining an on-site IT infrastructure with a hybrid cloud, that may be accessed over the Internet for a nominal fee. This paper is to study and understand Different cloud migration Models and all security concerns to be taken into account when the user wants to go for Cloud Migration. Even though the advantages of usage the cloud seems to be attractive, the enterprise decision-makers should also consider the security threats associated with cloud-service migration, thereafter have to take necessary precautions to overcome or to eliminate those security issues and perform a threat free cloud migration to ensure data confidentiality and completeness on the new Virtual Environment.

Keywords: Cloud Computing, Cloud migration Models, P2V Migration, V2V Migration, V2P Migration, Security Concerns of Cloud Migration

1 Introduction:

Cloud computing is not just a server that stores the data, but is something that offers a set of services such as storage, infrastructure, platforms, networks, and many more over the internet irrespective of geographical locations of servers and users as well. So any enterprise decision-maker may choose a CSP(cloud Service Provider) who is trustworthy and offer services at low cost. Here comes the concept of cloud service migration or Virtual to Virtual(V2V) migration. This migration model is referred to as the process of moving the Applications, Programs, software's, OS components and data from one virtual machine or disk partition to another virtual machine or disk partition of another Cloud Service Provider.

There might be different reasons for this kind of virtual to Virtual migration (V2V migration) from the customer's perspective. Customer may not be satisfied by the services provided by the present cloud Service Provider (CSP) and hence may want to move their data, applications, softwares and all IT infrastructure to another CSP. The present CSP seems to be untrustworthy to the customer and hence he may wants to migrate his data to another CSP. Cost might be another key constraint to the customer where a new CSP wants to provide same features with same level of security for lesser cost and/or the new CSP might provide more storage/services at the same cost. Whatever might be the reason once the customer decided to migrate from one Cloud to another cloud the first and foremost thing he has to think of is security concerns while migrating the data from one virtual cloud server to another virtual cloud server.

2 Cloud Migration Models:

Cloud migration is the relocating the existing on-premise data from the physical server to a cloud server which is controlled and monitored by the cloud service provider. The cloud migration methods are classified based on the source from which the data is being flit to the destination where the data is going to be preserved for further operations. The cloud migration is classified into 3 well known methods

1. Physical to Virtual cloud migration
2. Virtual to Virtual cloud migration and
3. Virtual to Physical Migration.

2.2 Physical to Virtual Cloud Migration:

Physical to Virtual Migration can be described as migrating and decoupling of all the data, applications, software and other IT resources from the physical server to a virtual machine hosted on virtual environment created and monitored by a cloud server.

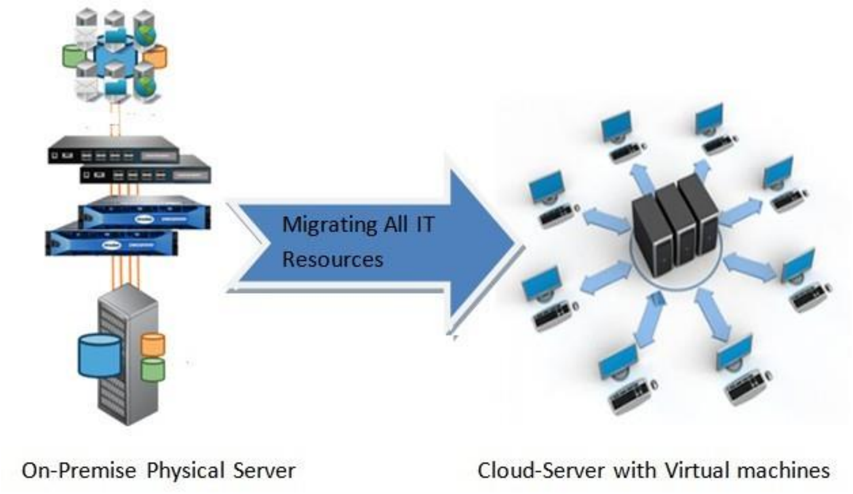
Migrating All IT Resources
On-Premise Physical Server
Cloud-Server with Virtual machines

Fig. 1. *Physical to Virtual Migration of applications and Organizational private Data*

All the It resources, applications, software and data is being created as an online copy and stored it on a virtual disk partition that is created. Now adopt the OS to the virtual hardware from raw virtual disk to the functional virtual disk and connect it to the virtual machine on the cloud server.

2.2 Virtual to Virtual Cloud Migration:

Virtual to Virtual (V2V) migration is a process of moving, transferring or replicating a virtual machine (VM), data or disk partition to another VM. It allows the migrating the data or a machine instance between VMs and/or virtual environment. To centralize the operation, some or all of the transferring data can be carried out necessarily by means of migration tools.

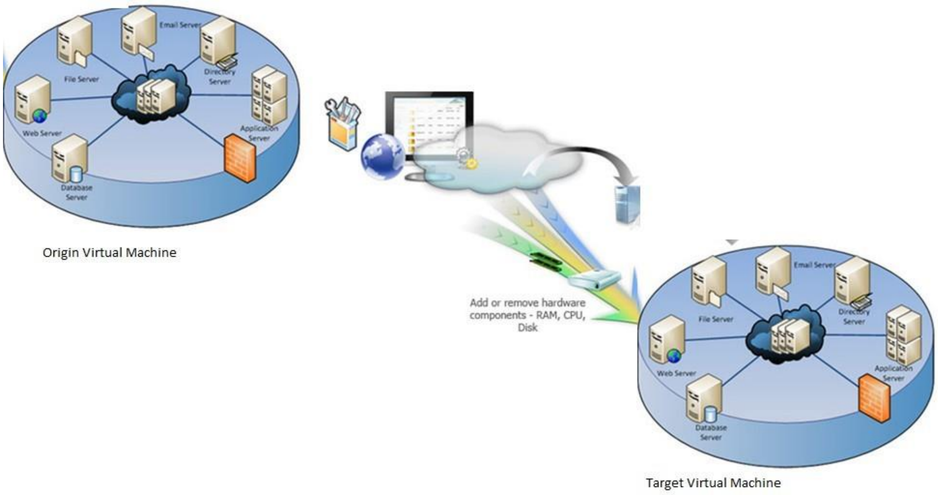

Fig. 2. *Virtual to Virtual Migration of applications and Organizational private Data*

There are many reasons for migrating data within the virtual/cloud environment. The following is a short list:

Storage upgradation: the existing storage frame is no more sufficient to store all the required data. Hundreds of terabytes of data is to be stored in the new Storage frames.

Consolidation of storage: Moving data from one storage to another in order to consolidate the storage space.

Performance tuning: Moving data from one storage to another in order to balance the distribution of active data onto separate storage spindles or controllers.

Regardless of the reason, VM images must be converted between the compatible virtual disk formats. Any V2V migration must be initialized with an assessment of the computing resource requirements of each original VM to ensure that those resources are available on the destination server. If not, the converted VM may need to be deployed on a different server, or other workloads may be redistributed to free the necessary resources. Migrating virtual machines (and the applications they're running) to the cloud can be cumbersome and complicated unless you use the right tools for the job.

2.3 Virtual to Physical Cloud Migration:

Virtual to physical (V2P) migration is the process of moving all operating system(OS), applications and data from a virtual disk partition to a computer's hard disk. Virtual to physical migration can be carried out manually by defining the target physical server such as a specific hard disk and then setup the applications, OS and data on it from the virtual Machine. This can be a boring and uncertain process, if the Destination server contains different hardware from the existing environment.

V2P can be used to reinforce the content of hard disk of a failed system or server from a backup storage medium such as a floppy or Tape or Disk drive. Virtual to Physical migration may be used, in conjointment with P2V migration, to copy the application programs, OS and data from one system to another virtual computer and from there to other machines. Worrying part of V2P because it could assist the progress of software piracy.

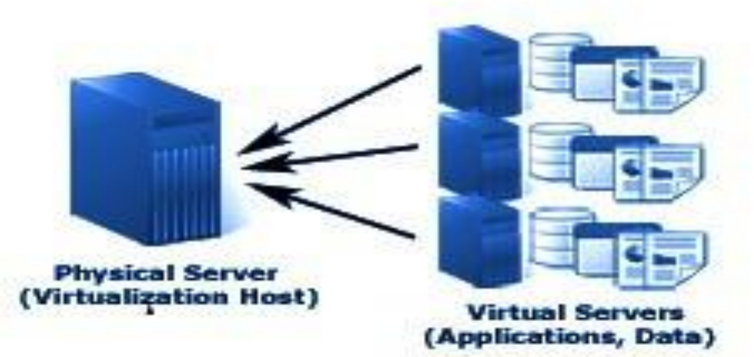

Fig. 3. Virtual to Physical Migration of applications and Organizational private Data

V2P is performed by a third-party tool external to the VM hypervisor and follows a systematic approach for successful migration. This includes verifying the hardware capacity and compatibility with a VM's current configuration. Required V2P tools include an operating system (OS) specific utility, which is used to create a VM image; an image transfer tool and native device drivers for the target physical machine. The OS tool that creates the OS image also facilitates the VM hardware setting configuration in line with the destination machine. The VM image/snapshot is copied exactly and configured by the same software and device drivers installed to complete the V2P migration process.

3 Security Concerns for Cloud Service Migration

3.1. Data Breaches

Cloud computing and services has evolved recently, yet data breaches in other forms have existed since long ago. A **data breach** is a scenario in which protected, secure or confidential data has been viewed, robbed or used by an unauthorized individual to do so. the data breaching might occur more likely for organizations that make use of cloud services than who don't. The outcome is that the cloud comes with a set of typical features that make it more susceptible. While we migrate the data from On-premise to Virtual or V2V migration or Virtual to Physical servers it is possible that some of the sensitive data can be viewed or accessed by unauthorized individuals.

3.2. Hijacking of Accounts

Attackers now have the ability to use organizational login information to remotely access important secure data stored on the cloud. Attackers may falsify and modify information through hijacked references. Other way of hijacking includes bug scripting and rehashing of passwords, that give a chance to attackers to detection steal credentials. during the Cloud migration process the attackers may falsify the data so that the target cloud service provider may not identify the data manipulation.

3.3 Insider Threat

An attack from inside of own company may seem unsimilar, but the insider threat do exist. Employees may use their *legitimate* access to cloud services provided by organization to exploitation or use information such as financial forms, customer details and other private information. Along with it these insiders need not to have intention to make the data malicious. The cloud migration process may also have insider threat hence it has to be done by trustworthy people.

3.4. Malware Injection

Malware injection is code or piece of program encapsulate into cloud services that resembles valid instances and run as Software as a Service to cloud servers. It means malicious script might be inserted to cloud and reviewed as segment of the s/w or service that runs within the cloud servers. Once an malicious data is executed and the cloud is operating in tandem with it, hackers may eavesdrop, agree with the integrity of secure data, and steal information. During the migration process insertion of malware or malicious code may be done without any being suspected.

3.5. Abuse of Cloud Services

The cloud service expansion has made it comfortable for both small scale and enterprise-level institutions to host large amount of secure data flexibly. However, the cloud's idiosyncratic storage capability has also allowed both authorized and unauthorized users to easily spread malware, software that are illegal, and other digital data. In some cases this becomes a hazard both the CSP(Cloud service Provider) and to their customers as well. During cloud migration process the attackers may them self add as authorized users so that from then onwards they can abuse the cloud services.

3.6. Insecure APIs

Application Programming Interfaces (API) give users the fortuity to personalize their cloud usage However, APIs can be a hazard to cloud security because of its nature. Companies allow the clients to customize features of their cloud services so that it suits their business requirements, but they also authenticate, give access, and performs encryption. As the framework of APIs improved to provide better service, its security risks also increased. APIs give developers the contrivance to develop their software to integrate their applications with similar job-oriented software. During cloud migration process the attackers may add new API's with which they may gain cloud access.

3.7. Insufficient Due Diligence

Many of the challenges we are focused here are technical issues, however particular security gap occurs when an company focus on clear goals, possessions, and policies for the cloud. Insufficient due diligence may cause security risks when an organization moves to the cloud without properly predicting that the services does not match client's assumption. It may interrupt the Migration process or allow the attackers the enter the cloud as authorized users.

3.8. Shared Vulnerabilities

Security in Cloud is a shared accountability between the cloud service provider(CSP) and its customer. The accompaniment between both of them cautions the client to take Preventive measures to protect their private data. The final conclusion is that CSP's and its clients have shared responsibilities, and ignoring your responsibility will result in compromising of personal data. The migration process is not an individual's responsibility and all the people involved are to be very cautious to avoid vulnerabilities.

3.9. Data Loss

Data placed over cloud may be lost through a venomous attack, natural disaster, or a data wipe by the cloud service provider. Losing essential information can be disastrous to those organizations without having recovery plan. Securing our personal data is nothing but carefully reviewing your provider's backup strategies as they relate to physical storage locations, physical access, and physical disasters. Even during the migration process the data may lost hence data validation has to be after completion of the migration to ensure the complete data has been migrated safely.

4 Overcome Cloud Migration Challenges

To move from a virtual data center to the public cloud with a variety of solutions are as follows:

- Control privileged user and super-admin access
- Guard against potential unauthorized copying
- Overcome the lack of visibility
- Mitigate the exposure of raw data
- Maintain ownership of your encryption keys
- Establish standard identity and data protection policies
- Demonstrate definitive proof of access and data control in compliance audits

5 Conclusion

Cloud computing is one of the highly thriving data storing and data sharing mechanism in the current computing environment. Cloud migration is the relocating the existing on-premise data from the physical server to a cloud server which is controlled and monitored by the cloud service provider. the different Cloud migration model are classified as P2V, V2V and V2P based on the source and destination data servers. The above mentioned security threats may cause great deprivation to organizational secure data. By being aware of security concerns, the migration team can build a cloud migration strategy to protect your business data, operating systems, application programs and all.

References

1. Cloud Migration Research: A Systematic Review|| by Pooyan Jamshidi, Aakash Ahmad and Claus Pahl, Member, IEEE
2. A Security approach for Data Migration in Cloud Computing , an International Journal of Scientific and Research Publications,Volume 3, Issue 5, May 2013 1 ISSN 2250-3153
3. Secure Migration of Various Database over A Cross Platform Environment, an International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013
4. Cloud Security Audit for Migration and Continuous Monitoring|| by Umar Mukhtar Ismail, Shareeful Islam School of Architecture, Computing & Engineering, University of East London,UK
5. S. Frey and W. Hasselbring, "The CloudMIG Approach: Model-Based Migration of Software Systems to Cloud-Optimized Applications", International Journal on Advances in Software, pp. 342-353, 2011.
6. C. Pahl, H. Xiong and R. Walshe, "A Comparison of On-premise to Cloud Migration Approaches - A Tale of Four Cloud Migration Processes," in European Conference on Service-Oriented and Cloud Computing , 2013.
7. Prashant Pant, Sanjeev Thakur, "Data Migration Across The Clouds", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013
8. V. Tran, J. Keung, A. Liu and A. Fekete, "Application Migration to Cloud: A Taxonomy of Critical Factors," in Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing, 2011.
9. V. Andrikopoulos, T. Binz, F. Leymann and S. Strauch, "How to Adapt Applications for the Cloud Environment: Challenges and Solutions in Migrating Applications to the Cloud," Computing, vol. 95, no. 6, pp. 493- 535, 2013.
10. Khadija SABIRI, Faouzia BENABBOU, "Methods Migration from On-premise to Cloud", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. IV (Mar – Apr. 2015), PP 58-65