Survey on Secure Live VM Migration in Cloud Computing by maintaining Integrity and Confidentiality

Punit K Mendapara[1], Prof. Sandip Chauhan[2]
[1]*M.E. Student, Department of Computer Engineering, Kalol Institute of Technology & Research Centre*
[2]*Assistant Professor,Department Of Computer Engineering, Kalol Institute of Technology & Research Centre*

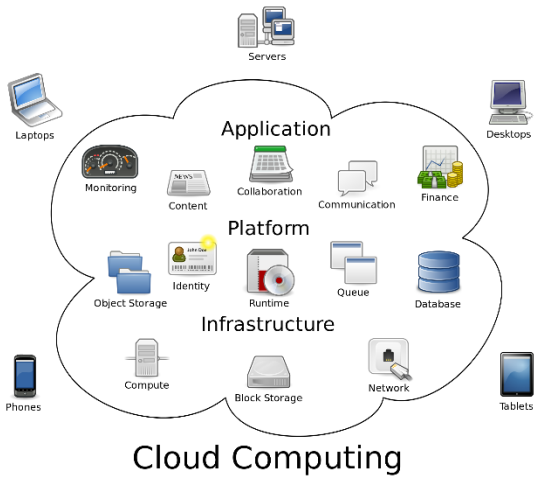
***Abstract*- Cloud computing is a new paradigm that combines several computing devices and technologies of the internet that creating a platform for more cost-effective business-consumer applications and IT infrastructure. With the increase development in the cloud computing environment, the Security has become a major concern as consumers look to move their data and applications to the cloud that the individuals do not trust the third party cloud providers while transferring with their important and private data. So the importance and motivation of security while the migration of VM on to the cloud and carry out an approach related to the security concerns with an encryption technique that provides both Confidentiality and Integrity in the migration of data on to the cloud. So here in this paper lookout the importance and motivation of security in the data migration in cloud and survey all the security approaches related to security in migration processes to cloud with the aim of finding the concerns, needs, aspects, requirements, benefits.**

***Index Terms*- Security; Cloud Computing; VM Migration; Encryption; Issues in Migration**

I. INTRODUCTION

Technologies like cluster, grid, and cloud computing have aimed at allowing access to large amounts of computing power in a full virtualized manner, by aggregating resources and offering a single system view. Cloud computing has been considered as term to describe a category of sophisticated on-demand computing services initially offered by commercial providers Amazon, Google, and Microsoft. It denotes a model on which a computing infrastructure is viewed as a "cloud," from which businesses and personal access applications from anywhere in the world on demand. The main principle of this model offers computing, storage, and software "as a service.[7]"

Cloud computing as "cloud can be said that it is a large set of easily usable and accessible virtualized resources like hardware, development platforms and services. The main aim of this to adjust to a variable load, allowing also for an optimum and maximum resource utilization. The study of presented in the paper is organized with a view to discuss and identify the approach to cloud computing and the security issues and concerns that must be



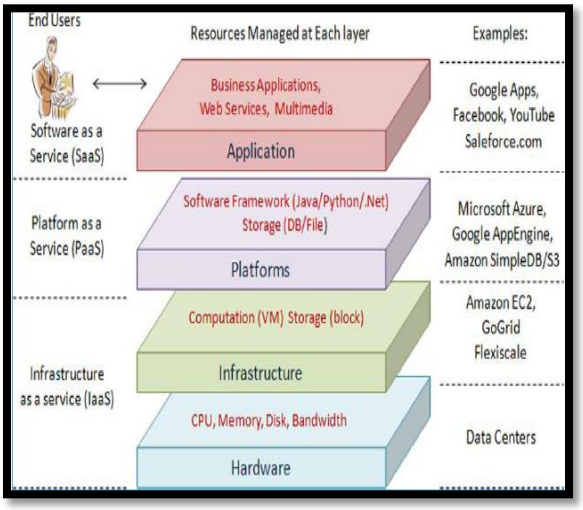
taken into account in deployment towards a cloud based infrastructure[9].

Cloud computing is prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. It is possible any unwanted party to 'sneak' on any private computers by means different ways of 'hacking'. The provision of widening the

scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result in center, security has always been an issue with cloud computing practices.

II. CLOUD SERVICES

Cloud computing services have three classes, according to the abstraction level of the capability provided and the service model of providers like (1) Infrastructure as a Service, (2) Platform as a Service, and (3) Software as a



Service[7].

A. Infrastructure as a Service (IaaS)

In this layer offering virtualized resources (computation, storage, and communication) on demand is known as Infrastructure as a Service (IaaS). A cloud infrastructure enables on-demand provisioning of servers running several choices of operating systems and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems.

B. Platform as a Service (PaaS)

In addition to infrastructure-oriented clouds that provide raw computing and storage services, another approach is to offer a higher level of abstraction to make a cloud easily programmable, known as Platform as a Service (PaaS). A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services (e.g., data access, authentication, and payments) are offered as building blocks to new applications.

C. Software as a Service (SaaS)

Applications reside on the top of the cloud stack. Services provided by this layer can be accessed by end users through Web portals. Therefore, consumers are increasingly shifting from locally installed computer programs to on-line software services that offer the same functionally. Traditional desktop applications such as word processing and spreadsheet can now be accessed as a service in the Web. This model of delivering applications, known as Software as a Service (SaaS), alleviates the burden of software maintenance for customers and simplifies development and testing for providers.

III. LOAD BALANCING IN CLOUD

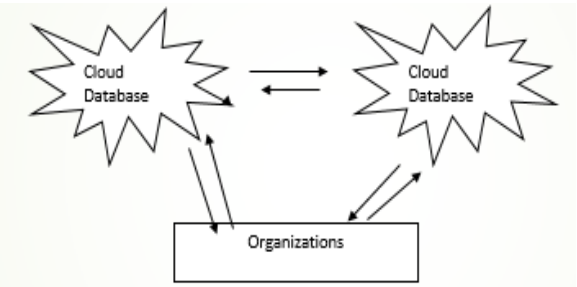
Load balancing is an optimization technique; it can be used to increase utilization and throughput, lower latency, reduce response time, and avoid system overload. Without load balancing, cloud computing would very difficult to manage. Migration service of virtual machines, is the process of moving a virtual machine from one server or storage location to another; there are many techniques of VM migration, hot/life migration, cold/regular migration, and live storage migration of a virtual machine.

Virtualization has termed technology by which a set of techniques and tools that facilitate the providing and management of dynamic data center. Virtualization is defined as the abstraction of computing resources like storage, processing power, memory, and network or I/O. One characteristic of cloud computing is virtualized network access to a service. Nothing matter where you access the service, you are directed to the available resources. The technology used to distribute service requests to resources is referred to as load balancing.

IV.VM MIGRATION & TECHNIQUES

In the Cloud Computing VM Migration is the method of moving a large amount of data and applications into the target cloud where the target cloud can be a public, a private or hybrid cloud. For that large numbers of applications are required to fulfill an organization's business needs and to improve its growth, various models of DaaS(Database as a Service) are now provided keeping in view the data migration process. The data can be migrated in several ways such as from any organization to a target cloud or from one cloud to another cloud. But it is quite challenging task to migrate data and it involves various major security issues as well like data integrity, confidentiality, security, portability, data privacy, data accuracy etc.[2]

VM Migration is required when an organizations or individuals change their computer systems or upgrade to new systems, or when system merge and load balancing. Also required when the organizations or individuals move their data from one place to another, within the same cloud or from one cloud to another cloud for some personal or business purpose.



1. Pre-Migration:

In pre-migration method some transformational activities are done previously before migration the data to cloud. This activities include server virtualization, data separation or server platform upgrades. The main purpose of this method is to make transformation easier by changing data into required format. So main advantage of this method is only those that make the migration easier, faster or less risky.

2. Post-Migration:

In this method, transformational activity is done after the migration has completed is a common requirement. Once the migration services have been successfully transitioned to the cloud, Data Centre Migration programmed should wind-down.

V.SECURITY ISSUES WHILE MIGRATION

At the time of data migration the most important concern related to this is Security. Thus, securing data remains an important priority of cloud managers to prevent global cloud security threats[1].

But it is quite challenging task to migrate data and it involves various major security issues as well likeseven security threats like Access Control, Authentication, Non Repudiation, Data Confidentiality, Data Integrity, Availability and Privacy have been analyzed and discuss in the context.

DATA SECURITY & MAIN TWO PROBLEM

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre.

Data security is also known as information security (IS) or computer security. Examples of data security technologies include software/hardware disk encryption, backups, data masking and data erasure.

1. Data Confidentiality

Data confidentiality is one of the pressing challenges in the ongoing research in Cloud computing. Confidentiality becomes a concern, data are encrypted before outsourcing to a service provider. Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it

access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories[6].

Sometimes safeguarding data confidentiality may involve special training for those privies to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.

2. Data Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent changes or accidental deletion by authorized users becoming a problem[5].

In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity.

Backups or redundancies must be available to restore the affected data to its correct state. The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity is imposed within a database at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines.

VI. RELATED WORK

A. Data Migration Across The Clouds[2]

In this paper show that With the ever increasing demands for the IT needs of businesses it is also important for data centers to deliver data migration cost effectively especially when faced with the demands from remote office back up, outsourcing, data center movers and cloud computing. Data management and migration are important research challenges of novel Cloud environments. This paper explores the issues and method of Data Migration across the Clouds. Also in this paper give the idea of which type of Data can be migrated.

B. Data Security and Privacy Protection Issues in Cloud Computing[4]

This paper introduced that Cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computingacross all stages of data life cycle. Then this paper discusses some current solutions.

C. Security approach for Data Migration in Cloud[3]

In this paper give the idea of the adoption of Cloud computing has been increasing for some time and the maturity of the market is steadily growing. Security is the question most consistently raised as consumers look to move their data and applications to the cloud. In this paper authors justify the importance and motivation of security in the migration of legacy systems and they carry out an approach related to security in migration processes to cloud with the aim of finding the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy system.

VII. CONCLUSION

From above discussion we concluded from the survey that the main cause of these vulnerabilities is insecure migration protocol and no single integrated approach is available which provide platform integrity verification, Confidentiality and Integrity of migration data, authentication and authorization of migration operations. For that at the time of Migration we have to consider many Security threats embedded in cloud computing approach are directly proportional to its offered advantages. The security issues could severely affect cloud infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer.

Now a days Cloud Computing is a growing because cloud provides users with access to high computational power at a fraction of the cost and also migrating enterprise applications and data within the cloud or over the another cloud. So many number of users are using cloud services but main problem arise while using cloud service it related to its security. But if the users decide to use the services of cloud, a number of threats arise and for that possible solutions need to be carried out to protect their applications, services and data from those risks and for that particular security reasons Encryption techniques are used and by using that technique we ensure the security of data.

REFERENCES

[1] Mahdi Aiash ,GlenfordMapp, Orphan Gemikonakli, "Secure Live Virtual Machines Migration: Issues and Solutions" , IEEE 2014 978-1-4799-2652-7/14 $31.00 © 2014 IEEE DOI 10.1109/WAINA.2014.35, 2014

[2] 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

[3] Virendra Singh Kushwah ,AradhanaSaxena, "A Security Approach for Data Migration in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May-2013

[4] Deyan Chen, Hong Zhao ,"Data Security and Privacy Protection Issues in Cloud Computing", 2012 IEEE International Conference on Computer Science and Electronics Engineering, 978-0-7695-4647-6/12 $26.00 © 2012 IEEE DOI 10.1109/ICCSEE.2012.193, 2012

[5] Mahesh S. Giri, Bhupesh Gaur, Deepak Tomar, "A Survey on Data Integrity Techniques in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 122 – No.2, July 2015

[6] Ms. Mayuri R. Gawande, Mr. Arvind S. Kapse, "Analysis of Data Confidentiality Techniques in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014

7] RajkumarBuyya, James Broberg, AndrzejGoscinski, "Cloud Computing Principles and Paradigms". Published by A John Wiley & Sons Publishing, Inc.

[8] Barrie Sosinsky. "Cloud Computing Bible", Published by Wiley Publishing, Inc.

[9] RajkumarBuyya, Christian Vecchiola, S. ThamaraiSelvi, "Mastering Cloud Computing". Published by Morgan Kaufmann Elsevier Inc.

[10] 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.

[11] 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.

[12] J. Sahoo et al., "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues" IEEE 2010.

[13]L. Shengmei et al., "Virtualization security for Cloud Computing service," IEEE 2011.

[14] Glenn Brunette, Rich Mogull, et, al. "Security Guidance for Critical
Areas of Focus in Cloud Computing V2. 1 ", Cloud Security Alliance,
2009.

[15] E. Stefanov, M. van Dijk, A. Oprea, and A. Juels, “Iris: A scalable cloud file system with efficient integrity checks,” in Proceedings of IACR ePrint Cryptography Archive, Tech. 2011.