“A STUDY ON VIRTUAL MIGRATION IN CLOUD COMPUTING”

A PROJECT REPORT

Submitted by

DHRUV PATHAK (190305105210)
PRAJESH PRAJAPATI (190305105217)
NEEL RATHOD (190305105230)

In fulfilment for the award of the degree

Of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE & ENGINEERING

Under the Guidance of

Prof.Umang Panchal

Assistant Professor

Computer Science &Engineering Department

Parul Institute of Technology

Parul University, Vadodara

2022-23

PARUL UNIVERSITY

CERTIFICATE

This is to certify that Project-II (203105400) of 7th Semester entitled "**A STUDY ON VIRTUAL MIGRATION IN CLOUD COMPUTING**" of Group No. PUCSE_60 has been successfully completed by

DHRUV PATHAK (190305105210)
PRAJESH PRAJAPATI (190305105217)
NEEL RATHOD (190305105230)

under my guidance in fulfillment of the Bachelor of Technology (B.TECH) in Computer Science & Engineering of Parul University in Academic Year 2022-2023

Guide name

Prof.Umang Panchal

Coordinator Name

Prof.Mohit Rathod

Name of HOD

Ms.Sumitra Menaria

Head of Department

CSE/IT/ICT

External Examiner

ACKNOWLEDGEMENT

Behind any major work undertaken by an individual there lies the contribution of the people who helped him to cross all the hurdles to achieve his goal.It gives us the immense pleasure to express our sense of sincere gratitude towards our respected guide **Prof.Umang Panchal**, Assistant Professor for his persistent, outstanding, invaluable co-operation and guidance. It is our achievement to be guided under him. He is a constant source of encouragement and momentum that any intricacy becomes simple. We gained a lot of invaluable guidance and prompt suggestions from him during entire project work. We will be indebted of him forever and We take pride to work under him.

We also express our deep sense of regards and thanks to **Ms.Sumitra Menaria**, Associate Professor and Head of CSE/IT/ICT Engineering Department. We feel very privileged to have had their precious advices, guidance and leadership.Last but not the least, our humble thanks to the Almighty God.

Place: Vadodara

Date:

ABSTRACT

Cloud computing has grown in prevalence from recent years due to its concept of computing as a service, thereby, allowing users to offload the infrastructure management costs and tasks to a cloud provider. Cloud providers leverage server virtualization technology for efficient resource utilization, faster provisioning times, reduced energy consumption, etc. Cloud computing inherits a key feature of server virtualization which is the live migration of virtual machines (VMs). This technique allows transferring of a VM from one host to another with minimal service interruption. However, live migration is a complex process and with a cloud management software used by cloud providers for management, there could be a significant influence on the migration process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 General Introduction

Cloud computing is the new computing paradigm which realizes the concept of computing as a utility where computing resources are offered as services and not as products. The rationale behind this concept is to provide computing resources to users over a network and allow them to offload the capital investment, management and operational costs associated with the computing infrastructure to a third-party, called the cloud provider. In this way, users can have adequate resources on-demand and overcome having constrained or excessive computing resources.

Cloud computing leverages server virtualization technology to form pools of computing resources from the physical infrastructure. Server virtualization is the virtualization technology that enables multiple virtual machines (VMs) to run on a single physical machine. This is achieved with the help of a hypervisor which abstracts the underlying physical resources. Server virtualization offers advantages such as server consolidation, dynamic resource management, hardware optimization, heterogeneous system operation, faster provisioning time and dynamic load balancing. Furthermore, cloud computing inherits one of the key features provided by server virtualization that is the migration of virtual machines.

Virtual machine migration is the process of moving a VM from one physical machine to another. VM migration has three different approaches, namely, cold, hot and live. In cold migration, the VM is shut down at the source, moved to the destination and restarted at the destination host. In hot migration, the VM is suspended at the source, moved to and resumed at the destination. In live migration, the VM remains in its execution state while moving it from source to the destination host.

This thesis focuses on live migration of VMs in the cloud. Live migration is a very powerful and handy technique for cloud and cluster administrators to keep up the Service Level Agreements (SLAs) with the users, such as maintaining average uptime, while carrying out tasks like:

- Load-balancing in order to relieve overloaded physical machines by migrating VMs to underutilized physical machines.
- Evacuating VMs from a server which is in imminent failure, requires maintenance, hardware or software upgrades.
- Optimizing resource utilization by consolidating idle VMs.
- Optimum VM placement, for example, to place the VM close to the storage cluster to reduce network and I/O latency.

1.2 Problem Definition

Live migration is an effective technique for optimizing the cloud infrastructure. The logical steps of the migration process using the pre-copy approach are shown in Figure 1.1. However, it is an inherently complex operation which becomes more complicated when there is a cloud management platform operating on the hypervisor and interacting with it for various operations including migration. Research works on VM live migration (Refer to chapter 3) focus mostly on optimizing live migration by either improving the memory transfer stage to reduce resource usage or by reducing the VM downtime. Moreover, there are various phases or stages in the migration process and each phase or stage will contribute to the total time taken for the migration process to complete. Modeling works either consider the total migration time without differentiating these phases or consider these phases to be constant or deterministic. By identifying and studying the performance of the migration phases, deeper understanding of the live migration technique can be obtained as well as better optimizations and modeling can be achieved

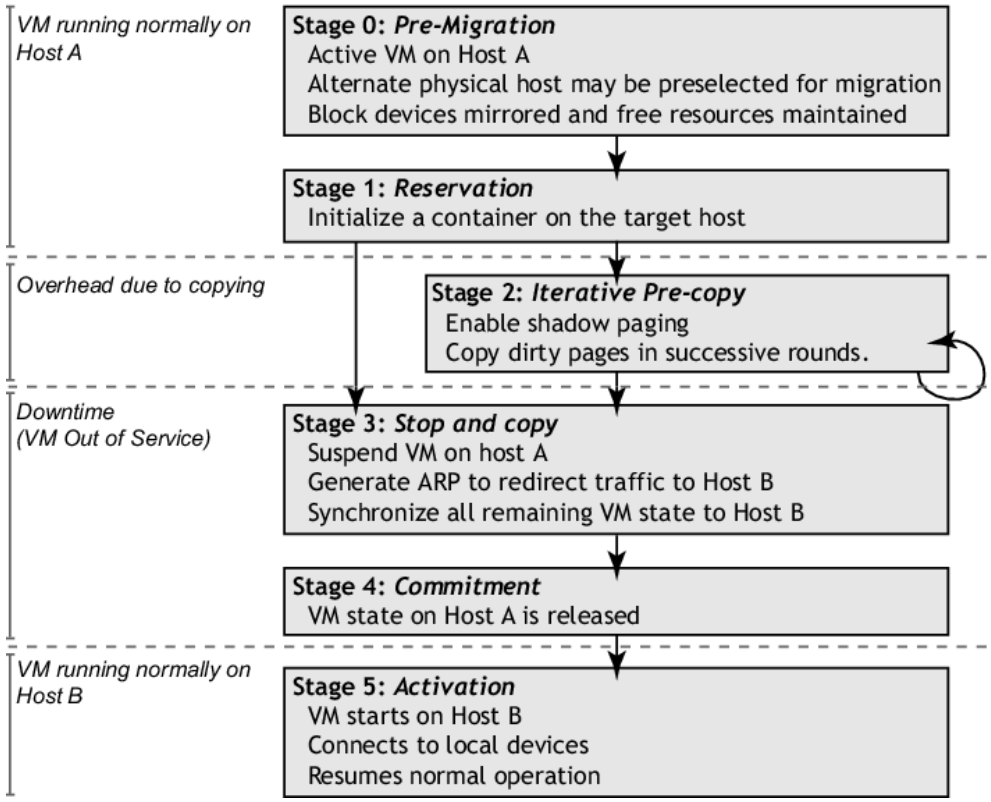

Figure 1.1: Logical steps of VM migration

1.3 Motivation

The growing adoption of cloud computing brought forward a new deployment model called a federated cloud. Cloud federation involves cloud providers collaborating together in order to share resources and act as a single cloud. One such federated cloud is the eXperimental Infrastructures for the Future Internet (XIFI) which is primarily deployed using OpenStack on Kernel-based Virtual Machine (KVM) hypervisors. It comprises of OpenStack cloud deployments from different regions around Europe of which Blekinge Tekniska Hogskola (BTH) represents the Karlskrona region. In such a deployment, the infrastructure computing resources from the cloud providers and application-level services from different user groups are managed securely using a central identity and authentication service, Keystone.

With respect to live migration, a remote Keystone adds latency for authenticating and authorizing the migration of VMs in the OpenStack cloud. This additional time depends on the relative location of the remote Keystone to the OpenStack deployment.

1.4 Objectives

The aim of this thesis work is to investigate the intricacies involved in the live migration process performed in a cloud scenario and analyze its performance. To accomplish this, firstly, we need to identify the sequence of events in the live migration process when performed by a hypervisor and when performed by a cloud management platform deployed on the hypervisors. This enables us to identify the additional steps executed by the cloud management platform. Secondly, we need to differentiate the phases of this process, measure and analyze their performance.

The cloud environment considered for this thesis comprises of the OpenStack cloud platform deployed on KVM hypervisors. The rationale behind this is the simplicity and power of OpenStack in administering clouds and most importantly, it is free, open source and easy to deploy using tools such as Mirantis Fuel. For the hypervisor, KVM has been chosen because it is free and open source as well. Moreover, it is the default hypervisor shipped with any Linux distro and OpenStack provides great support for KVM.

1.5 Scope of the project

1.5.1 Existing System

Organizations often face virtualization problems such as rampant virtual machines, network congestion, server hardware failures, reduced virtual machine performance, and software licensing restrictions. But companies can mitigate these problems before they happen with lifecycle management tools and business policies.

Here are the problems with virtualization:

- The spread of virtual machines: Consumes large amounts of computer resources.
- Network congestion: VM buildup can disrupt VM communication and cause network failures.

- Server hardware failure: Consolidating workloads into a single server may result in a single point of failure.
- Reduced performance of virtual machines: Older, internal, and custom applications may experience reduced performance with virtualization.
- Software License Restrictions: License violations can expose
- organizations to significant lawsuits and penalties.

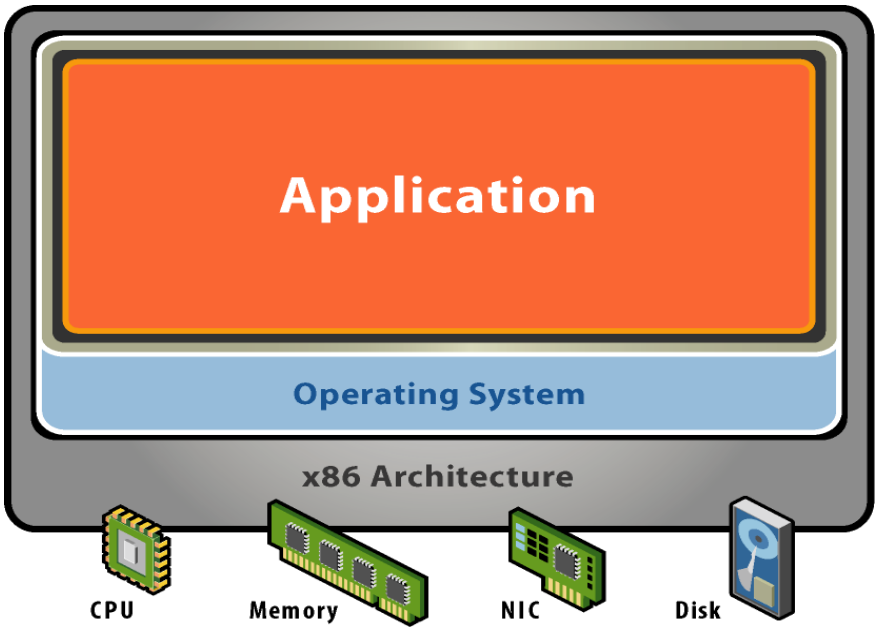

Figure 1.2 :Before Virtualization

1.5.2 Proposed System

From the technical view point, virtualization combines software and hardware engineered to create Virtual Machines (VM). VM is an abstraction of computer hardware that allows single machine to act as multiple machines. VM is required because a single OS can own all hardware resources. Contrary to this, VMs will enable multiple OS, each running on its own VM. Hence, the hardware resource is shared between many VMs each running its own OS. Virtualization offers cost savings for organizations that look for innovative methods to cut costs in IT without affecting business outcomes. From the technical perspective virtualization offers benefits in areas of consolidating server, storage and networks in the form of enhanced server efficiencies, improved disaster recovery efforts, increased business continuity and so on.

Here are the benefits with virtualization:

- Slash your IT expenses
- Reduce downtime and enhance resiliency in disaster recovery situations.
- Increase efficiency and productivity
- Control independence and DevOps
- Move to be more green-friendly (organizational and environmental)

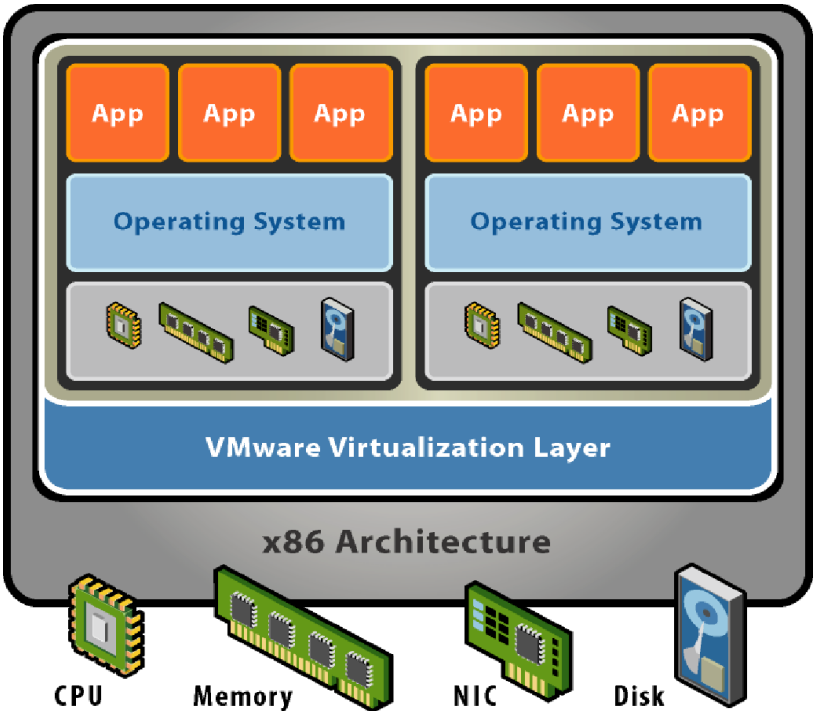

Figure 1.3 :After Virtualization

CHAPTER 2

ATTACK TYPE

2.1 Categories of DDoS attacks

From a cloud computing perspective. This examination is useful in In this section, we provide a categorization of DDoS attacks order to appreciate how the various DDoS attacks can impact the cloud environment and to be able to design effective detection mechanisms for the same. The well known categories of DDoS attacks are mentioned first.

DDoS attacks can be targeted towards depleting bandwidth or depleting resources of a network or a combination of both these approaches. The categories of DDoS attacks are: volumetric (Gbps), protocol (pps) and application layer (rps) attacks. Volumetric attack or floods target the bandwidth of the network and can be launched through botnets or amplification. Protocol attacks target the compute and memory of servers and interme- diate devices and often work at layers 3 and 4 of the OSI model on network devices like routers. Most attacks can be categorized depending on the vector and packet size, and the categories often overlap. Detailed description of DDoS volumetric and protocol attacks and their corresponding detection methods has been dis-Cussed.

2.2 Attacks on cloud infrastructure

The attacks on cloud infrastructure are as follows:

Flooding Attacks: It is a denial of service attack in which a service is put down by overwhelming it with a large amount of traffic. The attacker floods the target with incomplete connections which consumes resources of target, and as a result, the genuine packets are not processed. Examples of flooding attacks are ICMP Flood, TCP SYN Flood, UDP Flood, ACK Fragmentation Flood, HTTP Flood.

Carpet Bombing: It is a new variant of common flooding or reflection attack. Instead of attacking a specific IP address, theattacker attacks multiple systems which are a part of subnet or CIDR blocks. Flooding CIDR blocks also overwhelms the mitigation system. The other issue

is that detection systems usually rely on destination IPs but not on the subnets or CIDR blocks. This hinders the timely and accurate detection of attack.

Yo Yo Attack: This attack exploits autoscalability mechanism of cloud. The attacker sends periodic bursts of traffic which triggers the autoscaling process to alternate between scale up and scale down cycles. Rather than suffering from complete denial of ser-vice, the cloud users suffer from economic damage, i.e., the extra cost which has to be paid due to fraudulent packets causing the auto scaling process to scale up.

VM Sprawling: VM sprawling indicates the over abundance of resource draining VMs in the cloud environment, some of which may be obsolete. They are open to attack due to vulnerabilities that have not been patched up since the VM was last used.

Multi Vector: It is a new attack type in which the attacker combines different attack strategies to intensify the attack and make it difficult for systems to detect and mitigate the attack. The attacker may combine different types of flood attacks or may blend different amplification attacks or amplification attacks with traditional attacks.

Smurf & Fraggle: Smurf and Fraggle are amplification attacks. These attacks exploit the characteristics of broadcast networks. Smurf attack uses spoofed ICMP ping message to broadcast ad-dress, prompting each host to reply back, which further results in huge amount of traffic towards the victim. Similarly in Fraggle attack, the attacker sends spoofed UDP packets instead of ICMP packets.

CIDoS: Cloud Internal Denial of Service (CIDoS) attacks are those in which VMs attack their host with the help of covert channels. Each VM increases its resource consumption to disturb the host machine's ability to process the increase in resource usage. These attacks are harder to detect as the attack pattern is very similar to normal traffic.

2.3 Attacks on cloud services

The attacks on cloud web services and Software as a Service (SAAS) are as follows:

HTTP Flood: The attacker send legitimate HTTP GET or POST request towards the server. The attack GET and POST requests are similar to the normal HTTP requests. These volume of requests is so large that it consumes the resources of the target, leading to denial of service.

Billion Laughs: It is also known as XML bomb or exponential entity expansion attack. The attacker targets the XML parsers. The attacker may send a well formed XML message with schema validation which consumes the resources of cloud.

Cross Site Scripting: The attacker injects malicious JavaScript code into the targeted website. The code gets triggered when the user visits such websites. Upon execution of the code, the consumption of target resources jumps up, resulting in denial of the services running on the target.

Coercive Parsing: The attacker intentionally includes large number of namespace declarations, continuous open tags, deeply nested XML structures, which clogs up the CPU cycles.

NTP, Memcached DNS Amplification: NTP is a reflection based amplification attack in which the attacker exploits the functionality of NTP servers. The attacker sends spoofed requests towards the NTP servers which results in large response. Large number of such amplified responses consume the target resources, leading to denial of service. Similarly, in Domain Name Server (DNS) and Memcached amplification attacks, the attacker exploits DNS and Memcached servers for generating high volume and high bandwidth consuming DDoS attacks.

Oversized Encryption Attack: The attacker crafts the SOAP messages by including oversized digital signatures. These digital signatures when processed consume a lot of space in memory, leading to denial of service.

XML Attack: The attacker sends flood of XML messages towards the target. These messages are complex and parsing them is time consuming. The attacker manipulates some fields of XML message which eats up large resources of web services, ultimately breaking down the server.

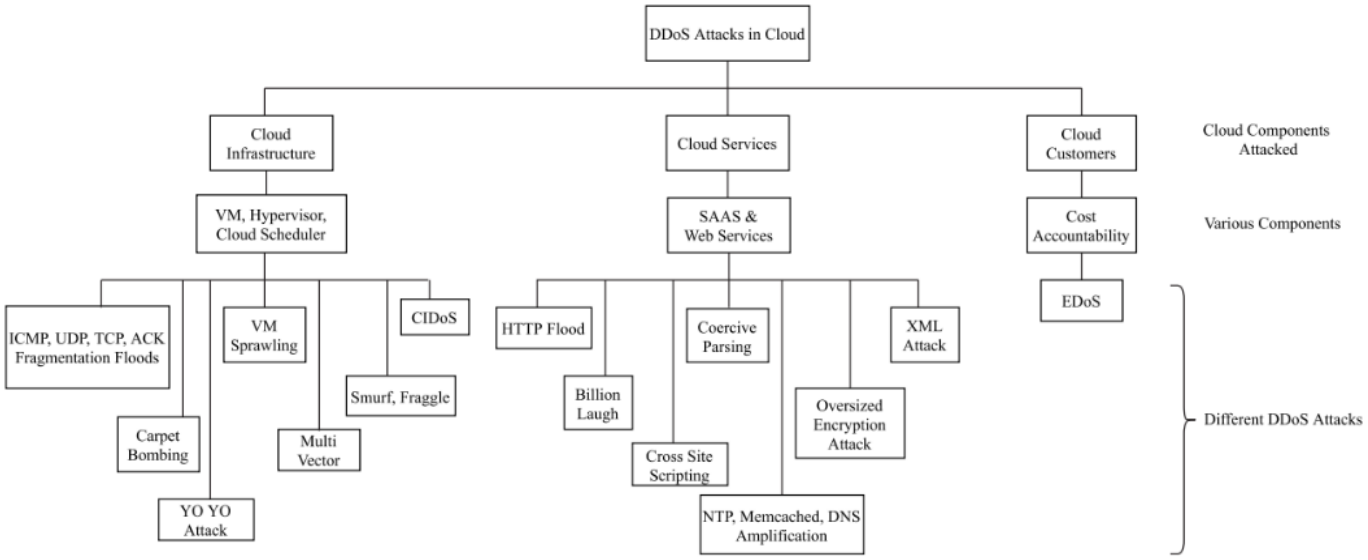

Figure 2.1: Categories of DDoS attacks in cloud.

2.4 Attacks on cloud customers

The primary attack that directly targets cloud customers is as follows:

Economic Denial of Sustainability (EDoS): DDoS attack is transformed to EDoS attack for cloud customers. The attack targets the economic resources of the customers by billing them for fraudulent resource consumption. The illegitimate usage of cloud resources is caused due to autoscaling of resources which has in turn arisen due to attack traffic, and not the customer's genuine traffic. This can lead to potentially infinite billing costs for the customer, leading to economic unsustainability for the cloud customer.

Inferences and Observations: At the network level, the most common attacks are TCP, UDP and ICMP floods, followed by reflective DNS, SNMP, SSDP floods. Fragmented packet attacks such as IP Fragment and TCP Segment are fairly common too. These attacks occur when reassembly of IP or TCP packet causes CPU saturation as packet is malformed with overlapping or missing values.They utilize very less bandwidth of attack/incoming traffic making them hard to detect. The common attacks at application layer are repetitive GET, low and slow attacks using Slowloris and its variants, slow read, and especially crafted stack/protocol/buffer attack.

CHAPTER 3

ATTACK DETECTION

3.1 Methods for detection of DDoS attacks

Classically, detection of DDoS attack can be categorized into three types: Signature based detection, Anomaly based detection and hybrid detection. Signature based detection technique uses a database of known attack rules. Traffic patterns are monitored for finding malicious events by comparing the patterns against the database. If the pattern is matched, the system raises alarm detecting attack. Signature based detection performs well in terms of detection accuracy if the database of rules is regularly updated. This technique fails to detect unknown attacks or zero-day attacks which leads to high false negatives. Maintaining an updated database of signatures is tedious and costly. The DDoS attacks employing botnets like leet and Mirai, are a prime example of cases where signature based detection methods are ineffective. These attack methods access local files and jumble or obfuscate their content to generate randomized payloads through millions of compromised devices. Since there is negligible similarity between packets, signature based methods are unable to detect an attack.

Anomaly detection refers to the identification of patterns that do not comply with expected behaviour. The terms ‘anomalies’ and ‘outliers’ are most commonly used, sometimes also interchangeably, in the context of computer networks. Anomalies may be point, contextual or collective. The network administrator prepares a baseline profile by recognizing network behaviour during non-attack period. The main aim is to observe or find subsequent patterns that vary from baseline profile.First, information of malicious and non-malicious traffic is collected and then it is sent to anomaly detection module fordetection of attack. On detection of anomaly, alert command is issued to network operator which mitigates or fixes the attack. Hybrid based detection method is a combination of anomaly based and signature based detection methods.

3.2 Inferences and observations related to DDoS detection methods

The major advantages of employing anomaly detection techniques for DDoS attack detection in cloud environment are:

- Anomaly detection techniques can detect new or unusual behaviours in the traffic in a timely fashion. This can help prevent or, at the least, control the potential widespread impact in terms of economic loss, reputation loss, service disruption, from affecting the multitenant cloud users.
- Anomaly detection techniques lower the False Alarm Rate(FAR) for known and unknown or zero day attack.
- It is difficult for attackers to know what actions can be carried out without getting revealed since baseline profile of normal behaviour is unknown to them.
- Anomaly detection directly leads to outlier detection, wherein a flag is raised whenever a user or server or entity is acting significantly different from other entities of its type at a given time.

The major challenges in adoption of anomaly detection techniques for detection of DDoS attacks in cloud environment are:

- Given the large number and variety of users in a multicloud environment, it is very difficult to define a normal baseline profile that includes every possible normal behaviour. User behaviour analytics is needed. Furthermore, it is strenuous to set a precise demarcation between normal and abnormal behaviour. The demarcation is more of a hyperplane than a line. Additionally, it is difficult to detect an event or reading that is close to the boundary as normal or anomalous.
- Anomaly detection needs to consider the variations due to different time periods and trends in the baseline profile, which is defined in terms of parameters like throughput, web requests, user logins, etc., while setting threshold values. Manually configuring alerts for these fluctuating values is a challenging task.
- Most of the anomaly based approaches build or learn a normal traffic activity profile or model and detect network traffic that deviates from baseline profile as anomaly. Thus, they are able to detect new attacks that deviate from normal traffic. False alarms can be a challenge for these techniques since any new and unseen traffic is

detected as an attack. Training on normal attack free datasets can help overcome this challenge. Maintaining an updated normal profile in evolving network conditions is a challenge for these techniques.

- Anomaly based detection systems may give high false positive rate when they encounter any legitimate but unusual upward surge in network traffic. For example, flash events are similar to high-rate DDOS attacks and involve a sudden increase in requests per VM, network bandwidth, response time, memory usage, etc. Additional information should be used to explain unusual behaviour that is not an attack.
- The anomaly detection technique must be application agnostic and in multicloud scenario, it should be cloud agnostic as well.
- There is a challenge of being able to identify anomalous patterns across multiple and multivariate network traffic streams.
- The sheer volume of data in a cloud environment poses a significant scalability challenge to anomaly detection in real time. Trillions of data points from several organizations and users of multitenant cloud need to be handled by the anomaly detection technique.
- The labelled data requirement for training and/or validation of system is generally a substantial problem.
- Traffic may contain noise that behaves in a similar way to the actual anomalies, and hence it becomes tough to differentiate and discard noise.

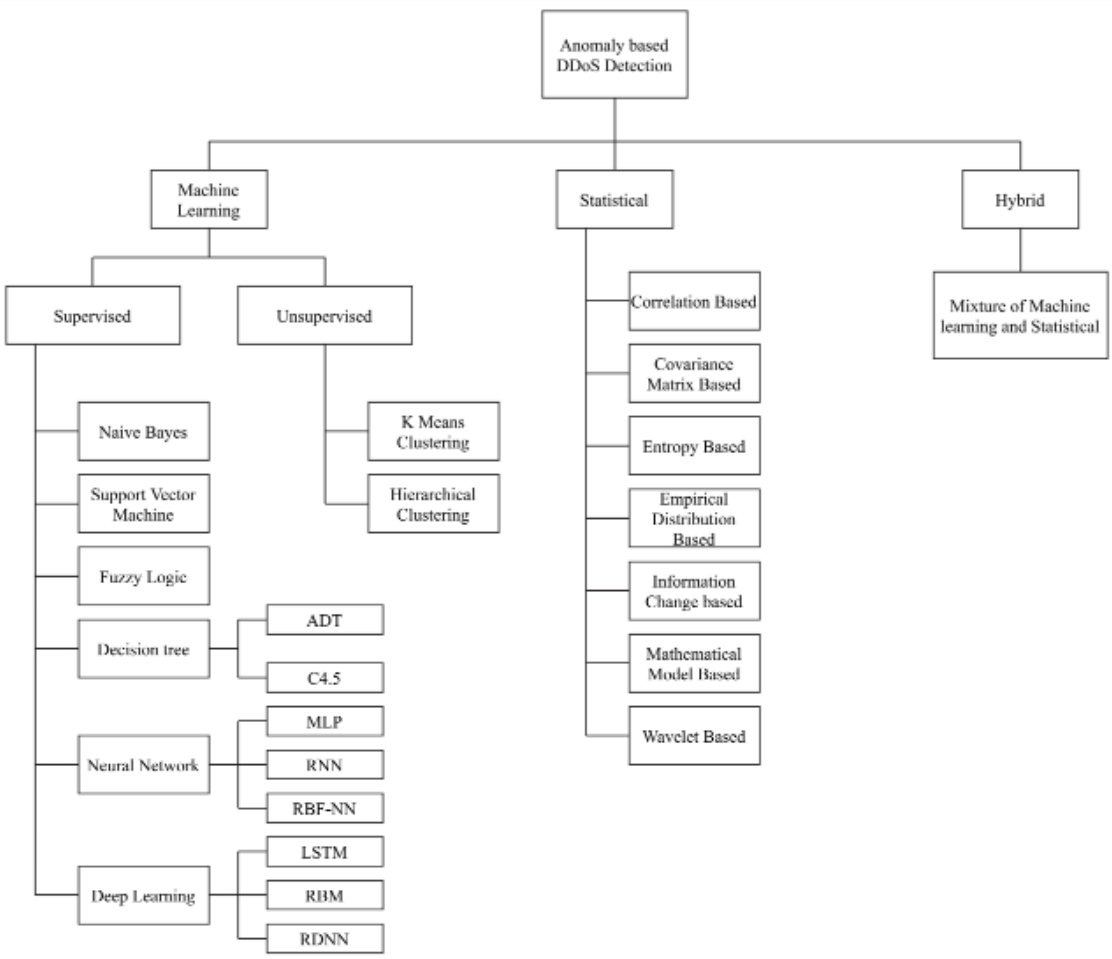

Figure 3.1:Anomaly based DDoS detection method.

CHAPTER 4

LITERATURE SURVEY

4.1 Survey

PAPER 1 :Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions

AUTHOR: Aanshi Bhardwaj,, Veenu Mangat , Renu Vig , Subir Halder , Mauro Conti

PUBLISHED BY: *University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India*

INTRODUCTION: Cloud computing provides an on demand computing paradigm to access services, resources and applications over the Internet. It has led to a shift in functioning of IT companies by moving from self-deploying and running of their daily IT facilities to using cloud computing platforms for infrastructure, storage, and other services. The National Institute of Standards and Technology (NIST) enumerates five key attributes of cloud, viz. services pro vided on-demand, resource sharing, ubiquitous network access, quick elasticity and pay as you go service

PAPER 2 : Mitigating Distributed Denial Of Service attacks: Network-Defence Methods

AUTHOR: Zhang Fu

PUBLISHED BY: Qualitative research(IEEE explore)

INTRODUCTION: Distributed Denial of Service (DDoS) attacks can be so powerful that they can easily deplete the computing resources or bandwidth of the potential targets. Based on the types of the targets, DDoS attacks can be addressed in two levels: application-level and network-level. Taking the network-based applications into consideration, a weak point is that they commonly open some known communication port(s), making themselves targets for denial of service (DoS) attacks. Considering adversaries that can eavesdrop and launch directed DoS attacks to the applications' open ports, solutions based on pseudorandom port-hopping have been suggested, where applications defend the attacks to the

communication ports by changing them periodically. As port-hopping needs the communicating parties to “hop” in a synchronized manner**.**

PAPER 3 : Handling System Overload Resulting From DDoS attack

AUTHOR: Zaid Al-Ali, Basheer Al-Duwairi, and Ahmad T. Al-Hammouri

PUBLISHED BY: Discussion(IEEEexplore)

INTRODUCTION: Distributed Denial of Service (DDoS) attacks can take several forms with different levels of sophistication, and remain very challenging to deal with especially those originating from botnets. Although botnet-based DDoS attacks can affect many different applications, the majority of them mainly target HTTP, where the aim is to exhaust the resource limits of Web services. Often, the attacks are customized to target a particular Web application by issuing requests that tie up resources deep inside the affected network. These attacks are typically more efficient than flooding attacks (e.g., SYN, ICMP, and UDP flooding) because they require fewer network connections to achieve their malicious purposes. Additionally, they simulate legitimate traffic making them hard to detect. Similarly, flash crowd events can unintentionally lead to denial of service because they usually result in server overload. The main difference between flash crowd events and DDoS attacks is that requests in a flash crowd events are originating from a large number of persistent legitimate clients who are eager to get some content from the Webserver, e.g., breaking news and stock market prices. CAPTCHA is a widely used technique to tell humans and bots apart, and has been proposed for DDoS attack mitigation. However, most CAPTCHA-based DDoS mitigation schemes propose handing CAPTCHA challenges through the Webserver itself (i.e., the victim) resulting in additional overhead on the server. As for addressing flash crowds, there have been also few proposed techniques to distinguish flash crowd events from DDoS attacks, e.g., or to handle flash crowd events, e.g., the HTTPreject system.

PAPER 4 : Migration Based Load Balance of virtual machines

AUTHOR: LUNG-HSUAN HUNG , CHIH-HUNG WU , CHIUNG-HUI TSAI, AND HSIANG-CHEH HUANG.

PUBLISHED BY: Theoratical research(IEEEexplore)

INTRODUCTION: Cloud computing is an Internet-based resource utility. Its central concept is ‘‘everything can be a service’’. In cloud computing, computing hardware and software

resources are capsulized as web-services that can be accessed through the Internet. Three application types of cloud computing models are defined: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Among them, virtualization is a representative IaaS application, which provides computing infrastructure resources, such as computing power, data storage, networking, all in the form of web services. IaaS providers purchase and maintain The associate editor coordinating the review of this manuscript and approving it for publication was Christian Pilato . physical computing and storage hardware and provide web services to users. With the virtualization technology, the users request IaaS providers for computation or storage resources as they own a ‘‘virtual machine’’(VM) without purchas- ing and maintaining physical hardware. The users can utilize VMs for deploying system/application software with a considerably lower cost of hardware procurement and possession.

PAPER 5 : An improved dynamic fault tolerant management algorithm during VM Migration In Cloud data center

AUTHOR: V.M. Sivagami, K.S. Easwarakumar

PUBLISHED BY: Qualitative research (sciencedirect)

INTRODUCTION: The infrastructure providers gain feedback via their deployment network virtualization technique in cloud infrastructure service. Several VMs could be employed in the individual physical server, and every VM could handle several application processes. This ensures that the server is effectively utilized in the aspect of reducing energy consumption. These VM based techniques lead us to enhanced levels of service multiplexing and resource utilization. Virtual Cloud Data Center (VCDC) consists of virtual machines, routers, and switches connected through virtual links with guaranteed bandwidth. Cloud Service Providers (CSP) achieves better performance isolation between VCDC and more effective resource allocation schemes are implemented. Energy consumption of cloud data centers is greatly reduced by applying virtualization technologies and the technology manages the overhead of accessible virtualized resources. At the same time, it also conveys the critical survivability challenges. It attracts many researchers to concentrate their study in the field of VN survivability. There are many challenges regarding cloud data center virtualization techniques such as migration, energy cost, load distribution, resource management, and survivability. Here, we consider VM survivability in case of node failures. In such cases, we

need to determine whether it is single node failure or multiple node failure. If it is single node failure, then we can optimize the VM within the intra-site server.

PAPER 6 : Design and Implementation of Virtual Machine Migration Method in Cloud Computing

AUTHOR: Shubhashish Goswami, Digvijay Singh, Sachin Sharma

PUBLISHED BY: Theoratical research (philstat)

INTRODUCTION: This paper provides an introduction to green cloud computing, which is a new type of cloud computing service. In the following section of this chapter, the basic architecture of green cloud computing is also presented. In addition, the major issues that this technology faces are briefly discussed. Within the green cloud computing scenario, the Virtual Machine (VM) Migration is discussed in the final section.

PAPER 7: A Load Balancing System for Mitigating DDoS Attacks

AUTHOR: ANDO Ruo, KADOBAYASHI Youki, MIWA Shinsuke, SHINODA Yoichi,

PUBLISHED BY: Theoratical research(ResearchGate)

I**NTRODUCTION:** Recent progress in CPU processor performance has allowed us to construct a virtual environment in which multiple operating systems (OS) run simultaneously. In particular,virtual machine monitors, which were used in the heyday of mainframe computers in the 1960s, have made a comeback in practical use with innovations in processor technology within the past few years. Virtual machine monitors are effective in streamlining resource utilization, load balancing, failure recovery, and reducing energy consumption. The present paper illustrates a strategy for mitigation of DoS (Denial of Service) attacks, which have come to pose a serious threat to current info-communication infrastructures, using virtual machine monitors.

PAPER 8: A Survey on Virtual Machine Migration:Challenges, Techniques and Open Issues

AUTHOR: Fei Zhang, Guangming Liu, Xiaoming Fu, Ramin Yahyapour

PUBLISHED BY: Theoratical research(ResearchGate)

INTRODUCTION: VIRTUALIZATION technology divides a physical server into several isolated execution environments by deploying a layer (i.e. Virtual Machine Manager (VMM) or hypervisor) on top of hardware resources or operating system (OS). Each execution

environment, i.e. Virtual Machine (VM), independently runs with an OS and applications without mutual interruption on each other. At the beginning, virtualization technology was not widely used due to a variety of reasons. For example, it will occupy a portion of hardware resources (CPU and memory). Furthermore, the poor network bandwidth also hindered vendors to lease their idle physical servers to clients. As the related technologies evolve, such as the utilization of Fibre Channel (FC) , the improvement of hardware performance, the development of security technology, etc.

PAPER 9: Maintaining Cloud Performance Under DDOS Attacks

AUTHOR: Moataz Hassan Khalil, Mohamed Azab, Walaa Sheta, Adel Said Elmaghraby

PUBLISHED BY: Journal(ResearchGate)

INTRODUCTION: A pay-as-you-go (PAYG) model is an innovative paradigm was designed by cloud computing providers to apply for application, platforms, services and computing resources to users. various Quality of Service (QoS) aspects, like performance, availability, and reliability are used to measure performance of different services provided by cloud computing platform. These performance metrics are explained in a Service Level Agreement (SLA) negotiated between users and cloud providers. Cloud services are classified as service as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS is a service of software deployment where a service is hosted as a service delivered to users across the Internet. SaaS is used to mention to business software rather than user software, which belongs to Web 2.0. without needing to install and execute a service on a user‘s computer it is considered as a way for businesses to get the same profits as commercial software with smaller cost outlay.

PAPER 10: Live Migration of Virtual Machines in the Cloud

AUTHOR: Sarat Chandra Pasumarthy

PUBLISHED BY: Qualitive research (Elsvier)

INTRODUCTION: Cloud computing is the new computing paradigm which realizes the concept of computing as a utility where computing resources are offered as services and not as products . The rationale behind this concept is to provide computing resources to users over a network and allow them to offload the capital investment, management and operational costs associated with the computing infrastructure to a third-party, called the cloud provider.

In this way, users can have adequate resources on-demand and overcome having constrained or excessive computing resources.

PAPER 11: Methods to Mitigate Attacks during Live Migration of Virtual Machines

AUTHOR: Joyce Beryl Princess, Getzi Jeba Leelipushpam Paulraj, Immanuel JohnRaja Jebadurai

PUBLISHED BY: Journal(SpringerOpen)

INTRODUCTION: Cloud computing enables the user to access services on demand over the internet. The services offered are platform, software and infrastructure. The users pay only for the services they access based on their requirements. The service providers promise a certain service level agreement to the client. This paper surveys various security threats during live migration and the methods to mitigate those attacks. Section II narrates formal methods for live migration of virtual machines from source physical server to destination physical server. Section III discusses various security threats during live migration of virtual machines. Section IV surveys various techniques to mitigate the security attacks during live migration of virtual machines. The comparison of various techniques was also drawn as a table. Section V concludes the paper with future work.

PAPER 12: An Analysis on Virtual Machine Migration Issues and Challenges in Cloud Computing

AUTHOR: K. K. Goyal , Vivek Jain , Pushpneel Verma.

PUBLISHED BY: Theoretical research (ResearchGate)

INTRODUCTION: Virtualization means multiple virtual machines on a single physical machine. Migration refers to the process of moving a virtual machine or application between different physical machines. A Virtual Machine is a complete computer system that is simulated in software and has complete hardware system functions and runs in an isolated environment. In cloud computing Physical machines hosts several Virtual machines from different customers to enable resource sharing that allows customers to use infinite computing resources on-demand. Virtual machine migration is a decision making process of selecting a destination server to full fill the customers requirement and provide efficient services.

PAPER 13: Optimization of live virtual machine migration in cloud computing

AUTHOR: Mostafa Noshy, Abdelhameed Ibrahim, Hesham Arafat Ali

PUBLISHED BY: Journal (SpringerOpen)

INTRODUCTION: Cloud computing depends basically on a major technology called virtualization. That technology was started in the 1960s by IBM as a transparent way to provide interactive access to mainframe computers, where time-sharing and resource-sharing allow to multiple users (and applications) to use huge size and highly expensive hardware concurrently . Nowadays, rapid technological development of processing power and storage has made computing resources more and more abundant, cheaper and powerful than before. Thus ,cloud computing trend has emerged due to this development, where computing and storage resources can be delivered to multiple users over the Internet in an on-demand fashion. Therefore, modern cloud computing environments can exploit virtualization technology to increase resources utilization and reduce both computational and energy costs. Virtualization technology allows running multiple operating systems (OSs) on a single physical machine with high performance. Each OS runs on a separate Virtual Machine (VM), which is controlled by a hypervisor.

PAPER 14: A critical survey of live virtual machine migration techniques

AUTHOR: Anita Choudhary, Mahesh Chandra Govil, Girdhari Singh, Lalit K. Awasthi, Emmanuel S. Pilli and Divya Kapil.

PUBLISHED BY: Journal (SpringerOpen)

INTRODUCTION: In recent year's IT resources become more powerful, having high processing capabilities and a large amount of storage capacity, which attracts the application developers and service providers to use these resources. Further, the increasing demand for IT resources motivates the researchers and providers to share these resources among end users for efficient utilization and maximize the provider's profit. In cloud computing environment services are delivered in the form of hardware, software, storage, platform, infrastructure, database and much more using Google's App Engine , Microsoft Azure, Amazon's EC2, IBM SmartCloud , etc. Cloud Computing delivers hardware and software capabilities in the form of services over the internet and allows consumers to be provisioned resources on-demand, on a pay-per-use model.

PAPER 15: Efficient virtual machine in cloud computing

AUTHOR: Hiren B. Patel , Megha R. Desai.

PUBLISHED BY: Theoratical Research(IEEE explore).

INTRODUCTION: Cloud computing establish number of remote software networks and servers that allow centralized data storage and provides on-demand network access to computing resources(e.g. storage, networks, servers, services, applications). Cloud model contains five essential characteristics (on-demand self-service, broad network address, resource pooling, rapid elasticity, measured service), three service models (software as a service, platform as a service, infrastructure as a service), and four deployment models (public, private, community and hybrid). Rest of the paper is organized as follows: Section II discuss the theory background for migration. Section III gives information about related work regarding to various techniques to optimize migration process. Section IV provides proposed approach finally concluded with future work in section V.

Sr No.	Title	Type Of Source	Purpose	Summary Points	Limitations
1	Distributed Denial Of Service Attacks in cloud[1]	Theoratical research (sciencedirect)	State of art of scientific and commercial solution.	Major Ddos incidents, attacks in IOT, categories of Ddos attack, Cloud stimulation related framework.	-the server slows down and service gets disrupted -no standard test bed or platform for IoT security.
2	Mitigating Distributed Denial Of Service attacks: Network-Defence Methods [2]	Qualitative research (IEEEexplore)	Application design and network defense.	Denial of capability(DOC), Sink tree architecture,	-effectiveness-overhead trade-off by addressing the issue of granularity of control in the network.
3	Handling System Overload Resulting From DDoS attack[3]	Discussion (IEEEexplore)	Flash crowd events	Security purpose CAPTCHA - identify human and bot, HTTP predirect module	-Do not have enough resources or infrastructure in place.

4	Migration Based Load Balance of virtual machines[4]	Theoratical research (IEEEexplore)	Load prediction using genetic based methods	Large scale management architecture, metaheuristic algorithms, Load balancing mechanism-VMH-GPE-	-migration is a job assignment optimization problem -usually a time consuming
5	An improved dynamic fault tolerant management algorithm during VM Migration In Cloud data center [5]	Qualitative research (sciencedirect)	Fault tolerance management algorithm.	DFTM algorithm, Cloud survivability, minimal complexity, recovery mechanisms.	-Poor Reliability -Collateral damage -Under-utilization
6	Design and Implementation of Virtual Machine Migration Method in Cloud Computing[6]	Theoratical research (philstat)	Green computing and maximizing proper utilization of resources using ACO	Cloudlet, ACO, Migration, virtual machine.	-By lowering server performance -power consumption and energy throughput have increased

7	A Load Balancing System for Mitigating DDoS Attacks [7]	Theoratical research (ResearchGate)	Live Migration of Virtual Machines	Virtualization technology, Security, Denial of service attacks, Live migration, Load balancing	-issue in info-communicatio n security, and preventive measures have generally consisted of installation of load balancing devices
8	A Survey on Virtual Machine Migration: Challenges, Techniques and Open Issues[8]	Discussion (ResearchGate)	Challenges, Techniques and Open Issues	Cloud computing, Data center, Virtual machine migration, Pre-copy, Post-copy, Hybrid-copy, User mobility, Performance analysis	- Termination conditions for pre-copy - Migration security - Multiple migration
9	Maintaining Cloud Performance Under DDOS Attacks[9]	Journal (ResearchGate)	Using MLD(Multipl e Layer Defense) Scheme for DDOS attacks	Cloud Computing, Energy consumption, Service Level Agreement, DDoS attack.	-With the MLD scheme, the number of VM migration reduces.

10	Live Migration of Virtual Machines in the Cloud[10]	Qualitive research (Elsvier)	Determine the influence of cloud management layer and analyze the performance	KVM, Live Migration, Measurements, OpenStack	-migration time increases with increasing VM flavor as well as has a slight increase with increasing CPU load.
11	Methods to Mitigate Attacks during Live Migration of Virtual Machines[11]	Journal (SpringerOpen)	Various mitigation techniques to reduce the security threats.	Cloud Computing, Hypervisor, Live Migration.	-migration time is very high in terms of pre-copy migration technique -the down time is high in case of post-copy migration technique.
12	An Analysis on Virtual Machine Migration Issues and Challenges in Cloud Computing[12]	Theoretical research (ResearchGate)	Analysis on VMs migration problems and challenges related to it	Virtual Machine, VM Migration, Cloud Server, virtualization, serial migration, parallel migration.	-The algorithms based on CPU utilization alone are less efficient for HighComputin g applications.

13	Optimization of live virtual machine migration in cloud computing [13]	Journal (SpringerOpen)	Optimizing the live migration on VMs	Virtualization, Hypervisor, Virtual machine, Live virtual machine migration, Downtime	-This large-sized data suffers from the heterogeneity of network architecture.
14	A critical survey of live virtual machine migration techniques[14]	Journal (SpringerOpen)	Focus to solve multiple virtual machine migration problem and load balancing	GCP cloud,less service downtime,pre copy techniques,post copy techniques	-public to private cloud vm migration is a challenging task .
15	Efficient virtual machine in cloud computing[15]	Theoratical Research(IEEE explore)	Managing efficiency by reducing transfer of duplications	Compression algorithm,Pre copy algorithm, Threshold value, multi-threding techniques	-no surity for reduction of downtime of low dirty page -not working with basic pre copy algorithm

Table 4.1 Literature review

4.2 existing system information based on literature survey

Advantages :

1. **Extremely Scalable :** The highlighting feature of cloud migration is beyond doubt its inherent scalability and flexibility , which is never bothered by changing one's

organization's periodic requirements. With cloud support you can plan without worrying about future IT infrastructure, and allocate resources accordingly.

2. **Better Storage -** Most organizations use cloud providers because they offer vast amounts of highly secure data storage at a fraction of the price it would cost them to store the data on premise. Also, you can easily expand and shrink your storage based upon your usage, which is extremely useful for businesses which see seasonal traffic.
3. **Automated Tasks -** With the help of cloud migration, your IT staff has less to worry about when it comes to keeping important business applications up to date. This is because all cloud applications are updated in the backend, without any interference, thereby resulting in improved organization-wide stability**.**
4. **Operational Flexibility -** A cloud solution allows you to be more flexible when testing and deploying applications. Your IT team does not have to install applications manually or through remote network individually since its deployed from the backend. Also, if you do not prefer an application, it can be easily removed and replaced with another one provided by your provider**.**
5. **Extensive Mobility -** A major advantage of cloud-deployed solutions for enterprises is the mobility that it offers for all your employees. Not only can they access important applications on the move if they have access to the internet, but also ensure that security is maintained even under uncontrolled conditions.
6. **Reduced Costs -** In today's competitive atmosphere, organizations worldwide are trying to cut their costs to remain profitable. Cloud migration helps them reduce both operating expense and capital expense by acquiring resources only when required and paying only for the same.

Disadvantages :

1. Cloud environment operate on new public and private IP which create complexity for new services. Which create complexity for new services. It is very difficult for migration tools to capture the configurations for Apache , tomcat etc.
2. Domain name system (DNS) services are outside the scope of migration. Even if the DNS name changes identifies tools may not allow flipping the switch to new location.

3. Migrating tools basically capture , translate and migrate security policy. It is very complex and even incompatible with cloud providers due to the dynamism in the changing security policies with respect to the time and cloud providers.
4. Complex load balancing policies may be problematic when migrating services to cloud.
5. Data transportation and synchronization create big problem when the data change continuously . So design of robust synchronization process is highly essential.
6. Frequently the configurations need to be modified manually in order to meet the advanced version of tools.

4.3 Algorithms(from the study based on the literature):

4.3.1 VM Load monitoring and balancing algorithm:

For all Service Request
While Task (Q. length) > 0 do
If received ACK from destination [T_id, T_ttl]
Change the Data Flow table in Switches
End if
End while
Set service rate of every request in the
service chain SR = 0.1 Service/sec
If SR > threshold (VM) then
Change the flow table SR
End if
End For
Select Request (Service_Chain(i))
Qmt = Service Request Removed from Chain on time
which is expected
Service transferred time = SnewSold (1 − a) + Slast X Δt
Δt = time adjustment values (0 < Δt < 1)
Snew = current average service request execution time
Sold = previous value service request execution time

Slast = the last service request execution time

Compute each host average response time (A)

The formula is: A = ((L + E + I + U) / L) ∗ R

- Advantages of proposed system:
    - **Performance Handling**
        - VM migration helps in increasing the performance of the machine by distributing the work load of a single machine to multiple machines
        - Sometimes too much load can decrease the performance of the machine so to overcome this problem we can use live VM Migration to distribute load of a single machine to multiple machines.
    - **Server Failure Recovery**
        - In case of server failure VM migration transfer user from the bad server to the working server with a very low amount of downtime
    - **Robust**
        - If one VM fail the other VMs will continue to work without any problem
    - **Energy Saving**
        - VM migration allows the users to save energy by combining the load of several server computers into one single physical unit (machine).
        - VM migration allows single machine to handle the workload of multiple machines
        - By handling the load of multiple machines the load of the other machines decreases hence less electric energy is used.

- **Security**

  - The data in one virtual machine is completely isolated from the other virtual machines which are running in the same physical machine

  - Data isolation safe data from viruses

  - If a data of single VM is attack by a virus the data of the rest of the VMs will not be affected by the virus because all VMs are isolated and separated from each other.

CHAPTER 5

METHODOLOGY

5. Methodology

5.1 existing methodology

5.1.1 LIVE MIGRATION STRATEGIES

Live migration is the process in which the hypervisor copies the state of the running source virtual machine to the destination virtual machine. Live migration is mainly performed using two methods, namely Pre-Copy and Post-Copy algorithm.

A.Pre-copy Algorithm

In Pre-copy algorithm the migration starts with copying memory pages from source to destination virtual machine while the processes continue to run on the source machine. The running process modifies some of the memory pages that are already transferred during migration. This process of writing over the transferred memory pages is called dirtying of memory pages. The dirtied memory pages are transferred from source virtual machine to destination virtual machine on iterations. The number of iterations depends upon the application running over the virtual machine. When the fixed round of copying is reached or threshold is reached the memory copying is stopped. In this instance the processes running over the virtual machine are suspended and its state and the remaining memory pages are migrated from source to destination virtual machine. The applications running over the virtual machines are resumed from destination server where the virtual machines are migrated.

The two main performance metrics measured during live migration are migration time, the total time required from the initialization of migration to activation of virtual machines in the destination virtual machine and downtime, the total time taken to stop and copy phase.

TotalMigrationTime= (Initialisation+Reservation)

Pre-migration Overhead

+∑Pre-copy+ Stop-and-copy

+(Commitmen+ Activation)

Post-migrationOverhead

TotalDowntime =Stop-and-copy

+(Commitmen+ Activation)

'Post-migrationOverhead'

B.Post-Copy Algorithm

The Post –copy technique initiates the copying of processor state and minimal memory pages of the virtual machine from source to destination server. The memory pages are fetched from the source virtual machine on demand. The demand is traced by generating page faults. The migration time is very high in terms of pre-cop migration technique and the down time is high in case of post-copy migration technique.

5.2 proposed methodology

1. Total Migration Time: It is the summation of all migrant VM's migration time. Its value can vary due to the amount of data to be moved during migration and migration throughput. It depends on

1) the total amount of memory transferred from source to destination server, and

2) allocated bandwidth or link speed.

$$t_m = \frac{v_m}{b} \tag{1}$$

Where, *t m* = total migration time

v m total amount of memory

b = bandwidth

2.**Downtime:** It is the time when service is not running or available due to migration of processor states. Downtime extends because current algorithms are not able to keep a

record of dirty pages of migrating VM. The downtime *t d* is depends on page dirty rate d, page size l, duration *t n* of the last pre-copy round n, and link speed b, Lui et al. define the downtime as:

$$t_d = \frac{d * l * t_n}{b} \tag{2}$$

3.Pages Transferred: The amount of memory contain by VM or number of pages transferred during VM migration, it also includes duplicate pages. Liu et al. [69] calculate the page transferred at round

$$v_i = \begin{cases} v_{mem} & \text{if} \quad \text{i} = 0 \\ d * t_{i-1} & \text{otherwise} \end{cases} \tag{3}$$

where, *v mem* : the amount of VM memory

t i−1: time taken to migrate dirty memory pages, generated during just previous rounds

The elapsed time of VM migration *t i* at each round can be calculated as:

$$t_i = \frac{v_{mem} * d^i}{r^{i+1}} \tag{4}$$

network traffic *v mig* during VM migration:

$$v_{mig} = \sum_{i=0}^{n} v_{mem} \left(\frac{d}{r}\right)^i \tag{5}$$

where, r: memory transmission rate during VM migration.

migration latency *t mig* is calculated as:

$$t_{mig} = \sum_{i=0}^{n} t_i \tag{6}$$

4.Preparation Time: The time difference between initiation of migration and transferring the VM's state to the target server, while continuing its execution and dirtying memory pages.

5.Resume Time: The time when VM migration is done and resume its VM execution at the targeted server.

6.Application Degradation: Due to migration the performance of application is interrupted or slow down services during migration

7.Migration Overhead: There is need of some extra machine resources to perform a migration.

8.Performance Overhead: Degradation of service performance during migration or interrupting the service while executing smoothly The migration process introduce delay, extra logs, and network overheads during applications execution on VM.

9.Link speed: It is the most crucial parameter with respect to the performance of VM. The allocated bandwidth or capacity of the link is inversely proportional to service downtime and total migration time. The faster transfer requires more bandwidth, hence it takes less total migration.

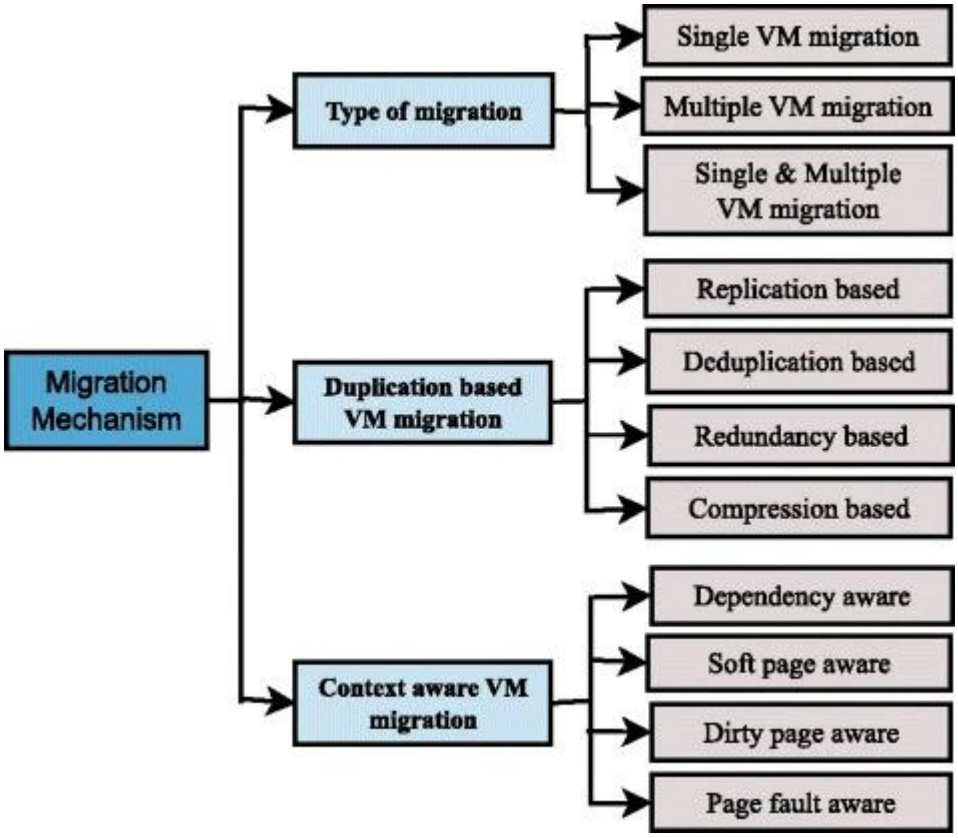

Figure 5.1: Classification of migration mechanism

During the process of migration, VMM detect multiple copies of the same page on single VM or Multiple VM's or on a number of different servers, that leads unnecessary memory pages

migration. For handling a large number of pages during migration requiring more network bandwidth or increase network traffic. Different type of memory compression techniques is used.

1.Replication based

2.De-duplication based

3.Redundancy based

4.Compression based

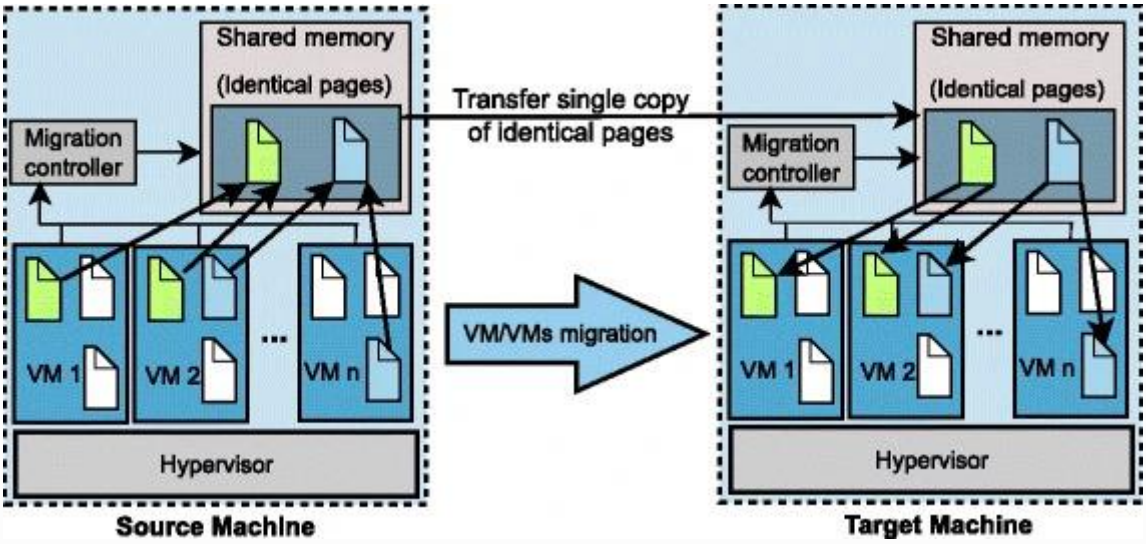

Figure 5.2:Generic steps of single/multiple VM migration

- Methodology

  1. Implement live migration of VMs with shared storage on the KVM hypervisor and OpenStack deployed on KVM hypervisor scenarios.

  2. Identify the sequence of events in the VM migration process in both the scenarios

  3. Construct a timeline of these events, categorizing them into phases, for both OpenStack and KVM-alone scenarios.

  4. Determine the performance of the migration phases with varying VM factors and workloads and analyze this performance.

CHAPTER 6

FUTURE SCOPE

VM Migration SLA Based-

There is a limitation of vm migration technology, when it is used for SLA (Service level Agreements) the optimized data access might still go beyond the time requirement.

High Dirty Rate Memory Page -

The problems like more page fault and higher total migration time occur when high dirty rate of memory pages even memory threshold technique applied.

CHAPTER 7

CONCLUSION

This paper presents techniques of live migration of virtual machine. Live migration includes transfer of a running virtual machine over physical hosts. There are many techniques which are used to minimize the down time & total migration time to provide better performance in low bandwidth. There is less number of network aware migration techniques available which helps more. With the increase in the popularity of cloud computing systems, virtual machine migrations across data centers and resource pools will be greatly beneficial to data center administrators. Live virtual machine migration is an indispensable tool for dynamic resource management in modern day data centers. In this paper presents the techniques of live virtual machine migration which takes considerable amount of migration time and downtime. Live migration of VMs should be designed in such a way so that downtime and migration time will be reduced.

REFRENCES

[1].https://www.sciencedirect.com/science/article/abs/pii/S1574013720304329

University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India 28 December 2020.

[2].https://ieeexplore.ieee.org/document/6377740

2011 Seventh European Conference on Computer Network Defense 06-07 September 2011

[3].https://ieeexplore.ieee.org/document/7371531

2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 03-05 November 2015

[4].https://ieeexplore.ieee.org/document/9374470

IEEE Access (Volume: 9) 10 March 2021

[5].https://www.sciencedirect.com/science/article/abs/pii/S0167739X18324208

Department of Information Technology, Sri Venkateswara College of Engineering, India 27 March 2019.

[6]Design and Implementation of Virtual Machine Migration …

https://www.philstat.org.ph › article › download

School of Computer Science & Engineering, DevBhoomiUttarakhand University, Chakrata Road, Manduwala, Naugaon, Uttarakhand 248017 19 July 2022

[7].https://www.researchgate.net/publication/294785868_A_load_balancing_system_for_mitigating_DDoS_attacks_using_live_migration_of_virtual_machines

Journal of the National Institute of Information and Communications Technology Vol.55 Nos.2/3 2008

[8].https://ieeexplore.ieee.org/abstract/document/8260891

IEEE Communications Surveys & Tutorials (Volume: 20, Issue: 2, Secondquarter 2018) 17 January 2018

[9].https://www.researchgate.net/publication/337838614_Maintaining_Cloud_Performance_under_DDOS_Attacks

International Journal of Computer Networks & Communications (IJCNC) Vol.11, No.6, November 2019

[10].https://www.diva-portal.org/smash/get/diva2:861751/FULLTEXT01.pdf

September 2015,Faculty of Computing,Blekinge Institute of Technology,SE-371 79 Karlskrona Sweden

[11].https://www.acadpubl.eu/hub/2018-118-21/articles/21d/92.pdf

International Journal of Pure and Applied Mathematics

Volume 118 No. 20 2018, 3663-3670

[12].https://www.acadpubl.eu/hub/2018-118-21/articles/21d/92.pdf

International Journal of Pure and Applied Mathematics

Volume 118 No. 20 2018, 3663-3670

[13].https://www.sciencedirect.com/science/article/abs/pii/S1084804518300833

Computer Engineering and Systems Dept., Faculty of Engineering, Mansoura University, Egypt 15 March 2018

[14].https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0092-1

Choudhary et al. Journal of Cloud Computing: Advances, Systems and applications07 November 2017

[15].https://ieeexplore.ieee.org/abstract/document/7280072

2015 Fifth International Conference on Communication Systems and Network Technologies 04-06 April 2015