Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

Capacity Building of Client-Server Disruption Network Over Cloud Server Using Network Forensics

Rohit Sansiya
Department of Computer Application
Maulana Azad National Institute Of Technology,
Bhopal, Madhya Pradesh, INDIA, 462003

V. Jackins
Department of Information Technology
National Engineering College,
Kovilpatti, Tamilnadu, INDIA, 628503

***Abstract*— Cloud computing is growing now-a-days in the interest of technical approach can be improved much instead of using traditional ICT. A significant number of secure systems are concerned with monitoring the environment. There are some equipment to measuring consumption of utilities but data loss can be a common experience of computer users, that lots of respondents had lost files on their home PC. The features included in Backup and Restore may differ depending on the edition of Windows. It is challenging for cloud providers to quickly interpret which events to act upon and the priority of events [8]. Unlimited host systems though realistically, you probably only need enough to host the number of VMs your license provides. Unlimited Virtual systems under management, So if you have a dozen real systems and they have Virtualization on them, you can manage all of them, without it effecting your Cloud hosted licensed virtual machine count. The server must also be granted permissions to make kerberos login just as they would if services creation was going to be done from client systems over disruption network and then administrator could be fetch the particular network using wireshark.**

Keywords: Security, Cloud computing, Network forensics, Centralized computing, Monitoring system

1. INTRODUCTION

Cloud computing has innovated information technology, enabling tasks formerly carried out by well-rounded computers and servers to be performed on a client-server disruption network such as lab. This new service delivery paradigm has the potential to become one of the most innovative developments in the history of centralized computing, so why not use this technology in your favor? Being available on the cloud and being independent of the device used, indeed, a pool of available resources such as applications, processes and services can be rapidly deployed, scaled and provisioned, on demand [13]. It is clear that security plays an important role in the acceptance of dealing with cloud computing where to put the data and run the software away from the user's location are a big challenge from the security aspect for many companies and users, also there are many possible problems resulting. The provider of service must have full right to use the server for the purpose of observing and preservation of the server [9]. We describe the design and implementation of the multiple-application client-server computing model that allows users with client devices to spread around a wide area network while facing a transparent working environment.

New discussions are indeed emerging, network forensic technology, on whether the cloud ecosystem could be adopted or even extended to tasks, Client-server disruption network can be applied to a variety of applications in WAN, such as centralized computing, cloud oriented infrastructure for an Internet service provider and monitoring system using network forensics. External Virtual Network Switches Disrupt Network connectivity and an Internal Virtual Network Switch allows communication between virtual machines connected to an internal virtual network switch and Hyper-V host [5]. Client-server disruption network can be applied to a variety of applications in WAN, such as centralized computing, cloud oriented infrastructure for an Internet service provide and monitoring system using network forensics. External Virtual Network Switches Disrupt Network connectivity and an Internal Virtual Network Switch allows communication between virtual machines connected to an internal virtual network switch and Hyper-V host [10]. A Private Virtual Network Switch can be used if you need to restrict communication between virtual machines connected to the same switch [1-3]. For instance, a peer-to-peer network has no central server. Each workstation on the network shares its files equally with the others if less number of systems connected with LAN.

The paper is well aligned with the networking proposals from both academia and standardization bodies to meet new cloud requirements. The authors have made an effort to assemble cloud resources and references and to present them at two levels; first, for those readers who are seeking to build knowledge on this topic; and second, for those seeking to progress their research.

2. PRELIMNARIES

The objective enlisting this section is to merge the details regarding preliminaries to make this paper self contained the study of cloud server in networking environment.

2.1. The Server-Side

The proposed solution assumes that information captured by the client-side, may be divided into smaller fragments and centralized process to the server-side platform to manage massive uploads more efficiently. The server-side will be responsible for acknowledging the fragments received and forwarding them to selected client using mechanism of centralized computing [12]. To allow forensic tasks, such as network forensics, be split and performed in centralized on one server, a forensic image can be considered as the natural unit of storage and processing. It is possible to run remote processes on a server capable of caching in RAM and processing image files, allowing complex forensic tasks to be quickly performed in centralized. The systems are the various computers, servers and data storage systems that create the "cloud" of computing services.

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity [11]. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems. As for web servers, it’s very easy to say, that if you are going to create a Windows based web server why not go with the include Hyper-V. It will shave off a lot from the cost of deployment as no additional licensing fee will be required for a commercial hypervisor.

The Microsoft’s Windows hypervisor is modeled according to Xen architecture. It is native to the Windows Server therefore, performs better in Windows environment. It alsosupports guest OS supported by hardware, but involves licensing issues. The data related to testing VMWare’s performance is greatly impacted by this factor on different parameters. It doesn’t have sharing memory block issues and is flexible with any kind of OS support. Another important feature to note in XenServer Hypervisors is its efficiency to manage performances varying from low, medium, and high loads that are commonly encountered in private cloud servers.

2.2. The Client Side

Client-side of the proposed platform, thought to be portable and very flexible. It is in charge of acquiring, dividing into independent fragments of smaller size and extracting documents of digital artifacts, in parallel, to the server-side platform, and sending consequently processing requests, based on the acquired data, to the server-side. In this architecture, the client contains presentation logic only, whereby less resources and less coding are needed by the client. It involves an intermediary (Application server) also known as middleware.

The client-side outlined above, in turn, is logically divided into two parts: a target-side, including a graphical user interface and the client software [14] [16]. The centralized computing between the server-side and the client-side is straightforward as it is possible to use the repository that can be used by both the server-side and client-side. The target-side i.e. client side, in turn, is responsible for reading the configuration scripts, executing them, collecting and writing results on OS [15]. The implemented solution avoids, therefore, complex protocol interactions and synchronization between the parties such as NETCONF and CoAP. It also happens critical servers, may not be powered-off or afford disruption to service, and must be analyzed with live forensic techniques. In a live forensic scenario, the target-side shall be able to:

I. Acquire current system backup an accurate time source

a. Physical memory dump, open files, open network connections, swap space.

b. Encrypted file systems where you do not have key to unlock

c. List of active processes

d. Windows registry

e. Temporary file systems

f. Message digests of gathered evidence

g. Active Directory

Parts of such requirements have been already implemented in the current release of the client-side. Dynamic resource assignment features make cloud on-demand schema possible. Operating systems and application frameworks are found in the platform layer. Applications are layered on top of whole hierarchy. Audit is introduced into computer systems by imitating supervisory mechanism in society, which is mainly applied to monitor system activities.

3. NETWORK FORENSIC INVESTIGATION

Network forensics is used to solve cyber crimes involving computers, networks or other IT components. If the communication between two networks a detailed analysis of this data is helpful to identify the further circumstances [20]. The combination of the retrieved outcome with any other branches of digital investigation like computer forensics, network forensic might improve the collective examination. the use of this techniques to collect, identify, examine, correlate from multiple, actively processing an transmitting digital sources for uncovering facts about the planned intent, or unauthorized bustle such as disrupt and compromise system as well as providing information to assist in response to or recovery from these bustle..

This can disrupt or demolish records and objects at server and client end. HTTP traffic analysis is increasingly by the ambiguous use of encrypted cloud containers by network traffic. Both types of traffic are frequently over application layer encryption mechanisms, generally using the ubiquitous TLS (SSL) protocol.

This activity on digital identification with authentication using LDAP provides privacy and liberty in new ways. Guest login security cannot protect privacy and security with such attitudes towards data. Privacy policy extends into all patch of society [17]. The challenge will be to establish the client server disruption model for state searches and seizures based on electronic evidence of questionable reliability. Currently, many internet service providers and websites are using OpenId to implement distributed SSO techniques. In this case, both user and service provider need to register to IdP in advance. During login, mobile user sends the adopted OpenId to cloud service provider, which in turn redirects it to IdP for verification of user authenticity [18]. This technique has two major issues.

As the United States v. Gourde court observed "We are acutely aware that the digital universe poses particular challenges with respect to the Fourth Amendment." That awareness still needs greater knowledge of the facts of identity and authenticity of electronic data as evidence, its mutability and evanescence, if the rights, liberties, and privacy of Americans are to be protected. Our requirements for the network environment was not limited to passive defense, so based on the current most popular cloud computing technology, a new generation of firewall technology, “coming with the clouds.

4. PROPOSED ALGORITHM TO MANAGE CLOUD SERVER

Let, Xi define XenServer and X is XenCenter who installed virtual machine (Vm) linux or RedHat (li) but the process for virtualization (Vi) controlled by X i and trying to virtualize the server for further proceedings. Now X i has the value in X i.e. (Xi == X) has n value for deploying by cloud server. There are so many media for storage enumeration in X based system. The way for installing and deploying technology as follows:

Step-1: For XenServer based Vm is an open source software is fully support OS linux on X86 hardware and 64bit size.

Step-2: During the process, we started working in Xen-Server with Static ip to connect the another system for virtualization.

Step-3: An another system connect with X is a open source software for bulding the virtualization technology. For CPU Utilization level

Step-4: In CPU storage, the all set is there, enabling the virtualization technology to set the system.

Step-5: An execution, the server turns to commend Vm in X. It means the all values of Xi turns to X (Xi == X)----(i) X has n value

Step-6: Disabled "Selinux' (Sx) (for brifging/ IP setup). In SElinux value depend on kernal. The value of kernal is (>1).

Similarly, [Sx > 0] Aspects of this algorithm namely CPU Storage, means CPU limits can be used to prevent a single virtual system from overwhelming others on the same host. For example, you might want each customer to be limited to 50% CPU, meaning that 8 such systems could run on a 4-core host without impacting each other. In SElinux value depend on kernal. The value of kernal is (>1). Similarly, [Sx >0]. This limit is typically expressed as a percentage, where 100% means the right to use a full CPU core.

On a multi-core host system, a limit could thus be set to more than 100%. It is also possible to turn off the CPU limit for a virtual system completely, which allows it to consume as much of the host's resources as it wants. Next phase is Memory level, in Xen systems always have a fix RAM limit, and do not allow that block to be shared with other systems while the Xen instance is running. Thus there is no possibility of over-committing RAM . V-server systems can also be configured with no RAM limit, which allows them to potentially consume all RAM on the host.

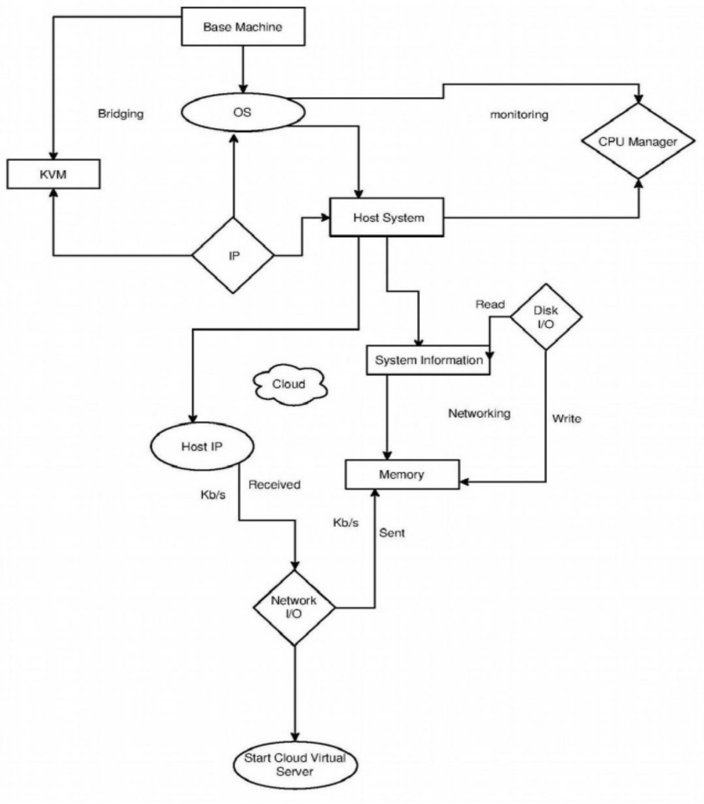


Fig 1.1 Block diagram for Managing Cloud Server

Memory that is not actually used by processes running within the system is potentially available to other virtual systems or processes on the host, which means that RAM can potentially be over-committed. When user creates a virtual system, the initial RAM limit can be set in the Resource limit options section of the creation form. In most cases, RAM available can be changed without needing to reboot the virtual system.

In all cases the new RAM limit will be saved in the appropriate configure file for the virtual system, and re-applied if it is rebooted. For instance, if an owner has a limit of 1GB RAM he could assign 512M to one system, and 512M to another. Next phase is Disk Input/Output, when Cloudmin creates a new KVM system, it will create a disk image typically with a single partition. This is then mounted as the root filesystem on the virtual machine. In some cases, there may be an additional partition that is used for the /boot file system. When Cloudmin creates a new KVM, it will also build at least one virtual disk whose contents are a copy of the selected system image. If you select to enable swap as well, another disk will be created for the swap file. In RPG Cloud Algorithm next phase is Network Input/Output phase, it requires that each virtual system have an IP address that is valid on the same LAN as the host system, which is typically a real Internet IP address. Each virtual system managed by Cloudmin has at least one network interface / IP address, which the system's hostname typically resolved to in DNS. Last phase of RPG Cloud Algorithm is Server Configuration level, means Achieving and IP configuration then check virtualization technology DNS is enabled or not. (for bridging connection). Network bridging connection or local host for GPL script installation in virtual server.

5. SYSTEM BACKUP AND RESTORE

There are two different types of backup supported: File backup and system image. File backups are saved to zip files. Two methods of file backup are supported: The first, normal backup, stores everything selected for backup. The second, incremental backup stores only files that are changed after a previous backup. The other method of backup, system image is a disk image of the backed up system saved block by block in a VHD file. Block-based backup is more efficient at performing subsequent differential backup, as only the blocks that have changed need to be backed up. Client-Server allows the master administrator and system owners to create backups of virtual systems running under Xen, Vservers. This provides protection against accidental deletion of files within the file system. Backups can be either run manually or on a regular schedule, such as once per day. When a backup is taken the virtual system can be either shut down to ensure a consistent file system state, or left running to avoid downtime Full backup idea is simple and easy to be implemented, but it needs a large amount of disk space.

Incremental backup usually only needs a little storage space but it is relatively complex. Moreover, considering the redundancy problem in incremental backup, data de-duplication and data compression technology are developed in recent years as a key solution to space efficiency problems of both storage and bandwidth intensive incremental backup systems. The proposed performance profiling model is used in conjunction with a cloud resource optimization scheme to ensure optimal performance. Our approach does not impose any requirements on the cloud platform other than providing isolated execution containers, and it alleviates the management burden of offloaded code by the mobile platform using stateful, autonomous application partitions.

In older versions backups only include the contents of the virtual system's file system or disk images. When backing up running KVM using LVM logical volumes to store disk images, LVM snapshots are used to take an instantaneous copy of the file system while it is copied. Each will consume 10% of the space in the volume group as the underlying disk images, so make sure you leave some LVM space free. Server can backup virtual systems to a variety of different destinations - via SCP, FTP or to any system it manages. In a typical Cloud based setup a single system with plenty of disk space is chosen as backup destination, perhaps the master system itself. Backups are taken on the host systems and then transferred to this backup machine. Alternately, you can choose to store backups on the hosts themselves, to avoid the need to transfer large backup files over the network.

When a backup is made it will be saved to the specified directory in a file whose name is that of the virtual system appended. Each subsequent backup of the same system to the same destination will overwrite that file. The entire disk or individual files can be restored through the utility. In addition, the VHD file can be attached (mounted) as a separate disk. Regardless of the latest backup being incremental or full, the attached disk will reflect the state of the disk at the latest backup, with the previous version's feature exposing older backup sets.

Client-Server logs all backups it performs, including their final status, systems included, disk used and possibly the complete progress report. To view logs, go to Backup and Restore -> Backup Logs, and enter a host name or destination path into the Find backup logs box, then click Search. The simplest way to restore a backup is to click on its destination in the search results, which will open a restore form. If the system no longer exists, the restore process will re-create it from details stored alongside the backup file.

5.1. System Backup

A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data detection. Data loss can be a common experience of computer users; a 2008 survey found that 66% of respondents had lost files on their home PC. The features included in Backup and Restore may differ depending on the edition of Windows. Only Windows Vista Home Premium, Business, Enterprise or Ultimate editions can schedule automatic backups or back up files and folders to a network location. Only Windows Vista Business, Enterprise and Ultimate editions support Complete PC Backup. Before data are sent to their storage locations, they are selected, extracted, and manipulated.

Also more data has to be stored. Having bigger size will be fast and need to be performed, but the chances of finding data duplicates will be less. So carefully choosing the data block size will provide the correct balance between the duplication ratio and centralized computing required. Fixed block size Deduplication is inefficient, if there is any change in the data, but it is less complex and not much intelligence is required.

Many different techniques have been developed to optimize and live data sources as well as compression and encryption. Every backup scheme should include validate the reliability of the data being backed up. It is important to recognize the limitations and human factors involved in any backup scheme. Any backup strategy starts with a concept of a data repository. The backup data needs to be stored, and probably should be organized to a degree. The organization could be as simple as a sheet of paper with a list of all backup media (CDs etc.) and the dates they were produced. By default, systems are backed up one by one. This will only work if the backup is to a date-based directory. To just show which systems will be backed up and to where use the flag. This is useful when selecting systems by group or host, or when using a date-based backup destination spec.

Each virtual server's backup is typically a single file in tar.gz format it contains one or more files per Virtual min feature that is included in the backup, such as the contents of databases, DNS records, Apache directives or the virtual server's home directory. It is also possible for a single backup file to contain multiple servers, although this format is generally not as easy to work with. This allows you to restore the state of an entire virtual server (including all databases, users and aliases), without effecting other parts of the system. A better alternative is to backup to another system, perhaps owned by your or maybe provided. The backup files can be transferred either via FTP or SSH, depending on which protocol the destination system supports. Almost all Unix systems will allow SSH logins, but some network attached storage devices will only support FTP. Another option is to use Amazon's S3 storage service, which charges you by the megabyte for data stored on their systems. This is probably the safest option as S3 presumably has backups of their own, but is more costly and slower to transfer backups to over the Internet. Alternately, you can backup to Rackspace's Cloud Files service. This is similar to S3, in that your backups are saved to storage managed by another company.

5.2.2. Server Monitoring And Auditing

Potential cloud computing consumers like to know whether the controls in cloud environments can adequately protect critical assets migrated into the cloud. We present a cloud security audit approach to enable users' evaluate cloud service provider offerings before migration, as well as monitoring of events after migration. Systems that depend on the existence of a particular sensor are less effective in IaaS environments. Although IaaS cloud environments introduce challenges above and beyond private data centers, the techniques for securing both environments are similar. Systems monitoring applies to institutional equipment, your personal equipment when accessing the Systems and the communications, information, and materials conveyed or accessed using the Systems. Monitoring activities may be conducted by automated means, sampling or manual reviews; and routinely or in connection with specific incidents, investigations. A privacy-preserving multi keyword ranked search approach over encrypted cloud data was proposed [19], which can search the encrypted cloud data and rank the search results without leakage of the user's privacy.

A significant number of secure systems are concerned with monitoring the environment. The monitoring application needs information such as log file path and number of threads to run with once the application is running, it needs to know what to monitor, and deduce how to monitor. Because the configuration data for what to monitor is needed in other areas of the system, such as deployment the configuration data should not be tailored specifically for use by the system monitor, but should be a generalized system configuration model. During the loop, devices are polled via SNMP calls, hosts can be accessed via Telnet/SSH to execute scripts or dump files or execute other OS-specific commands, applications can be polled for state data, or their state-output-files can be dumped.

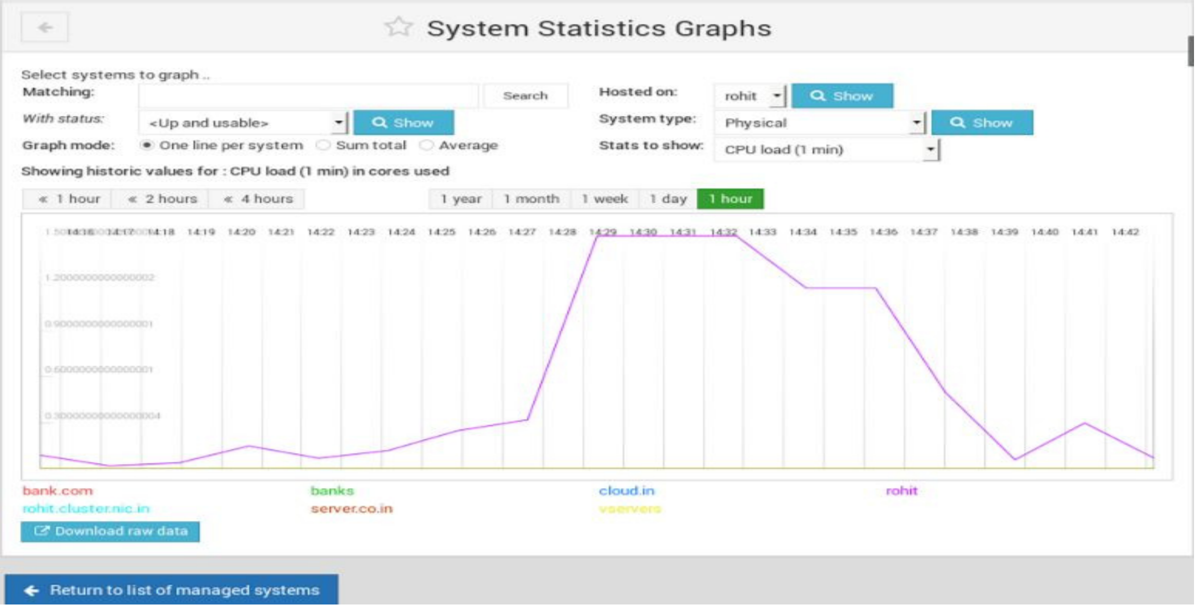
The main disadvantage of this mode is that the monitoring process can only do so much in its time. or instance, a CPU resource is further qualified as CPU idle, CPU user, which respectively correspond to the percentage of idle CPU, the CPU utilized by the system and the user. These concepts are considered as a language for describing the properties necessary for cloud security audit both before and after migration.

Customers with computer expertise may understand each parameter well, but for common customers, exhaustive monitoring information adds to the burden of analyzing system performance. Thus, it is essential to reduce the dimensions of monitoring data items. After getting lower dimensionality, we also need to aggregate data so that data in the same group will be more similar to each other than those in different groups. Monitoring plays an important role in cloud system management because of its impact on improving service quality, as well as planning for optimal capacity allocations in the various components of cloud systems, e.g. memory, disk, processors and cores, and network support. Besides, monitoring also helps in other aspects, such as resource utilization tracking and billing, troubleshooting, and security.

6. RESULTS AND DISCUSSION

A. CPU Load Time in Graph

Only the normal mode is critical with regard to CPU usage. In this mode, the connection is established, and the data transfer scenario is enabled. The data transfer scenario of the drivers for an example communication protocol is shown in Figure 1. Start monitoring CPU, Memory, and Disk utilization instantly.



System Statistics Graphs

Select systems to graph ..
Matching: Search
With status: <Up and usable> Show
Graph mode: ● One line per system ○ Sum total ○ Average
Hosted on: rohit Show
System type: Physical Show
Stats to show: CPU load (1 min)
Showing historic values for : CPU load (1 min) in cores used

Fig. 1(a) Graphically representation of CPU Load Time

- CPU Metrics (CM): The cpu metric group tracks CPU utilization for hosts, virtual machines, resource pools, and compute resources. The performance charts display a subset of the CPU data counters.
- CPU Idle (CI): Total time that the CPU spent in an idle state (meaning that a virtual machine is not runnable). This counter represents the variance, in milliseconds, during the interval.
- CPU Ready (CR): Percentage of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads.
- CPU Reserved Capacity (CRC): Total CPU capacity reserved by the virtual machines.
- CPU System (CS): Amount of time spent on system processes on each virtual CPU in the virtual machine. This is the host view of the CPU usage, not the guest operating system view.
- CPU Total (CT): Total amount of CPU resources of all hosts in the cluster. The maximum value is equal to the frequency of the processors multiplied by the number of cores. For example, a cluster has two hosts, each of which has four CPUs that are 3GHz each, and one virtual machine that has two virtual CPUs.

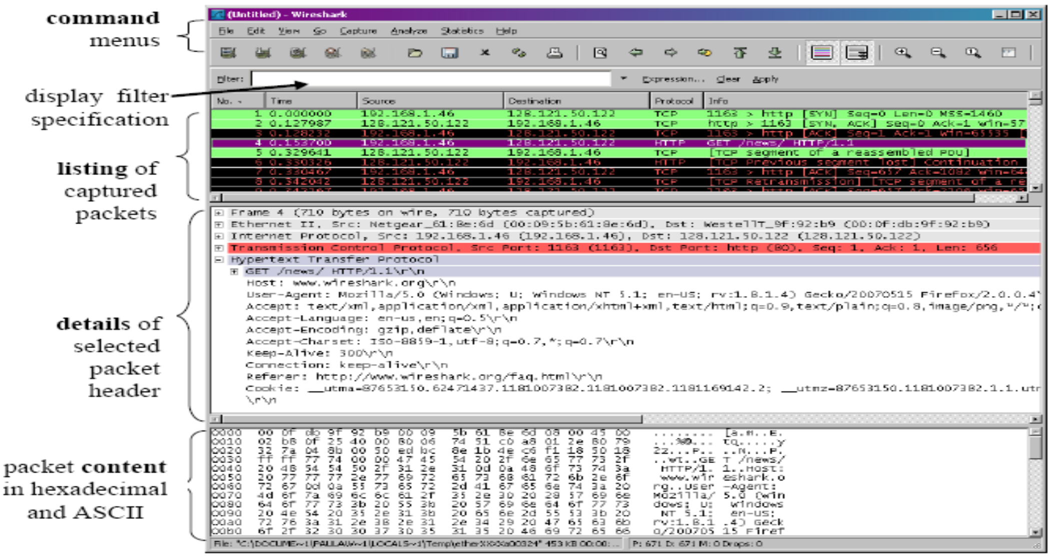
VM totalmhz = 2 vCPUs × 3000MHz = 6000MHz

Host totalmhz = 4 CPUs × 3000MHz = 12000MHz

Cluster totalmhz = 2 x 4 × 3000MHz = 24000MHz

B. The Analysis of Traffic of IP Packets using Wireshark

Malware and Software Vulnerability Analysis (MSVA): It is Open Source Network Tool. GUI for displaying tcpdump/tshark packet traces. We are often not interested in all packets flowing through the network. We use filters to capture only packets. It also discusses ways to detect the presence of such software on the network and to handle them in an efficient way. Focus has also been laid to analyze the bottleneck scenario arising in the network, using this self developed packet sniffer. The development of web server by using centralized architecture gives a chance to incorporate the additional features that are not in the existing one.
For example: Packets 1-30 are boot. Packets 31-500 are login. Packets 501 to 1,000 is my application loading. Packet 1,001 to 1,500 is my saving file. The error occurred at approximately packet 1,480. Larger traces should be uploaded to MANIT FTP server. Zip the traces and a readme.txt with a description of what you traced, using SRnumber.zip as a naming convention, e.g.2345678.zip. A common procedure for taking a trace is to get two traces, one of a workstation that works and one of a workstation failing. When doing this, it is important that the exact same steps are followed in each trace so they can be accurately compared.


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time       Source          Destination     Protocol Info
     1 0.000000   192.168.1.46    128.121.50.122  TCP      1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987   128.121.50.122  192.168.1.46    TCP      http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232   192.168.1.46    128.121.50.122  TCP      1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700   192.168.1.46    128.121.50.122  HTTP     GET /news/ HTTP/1.1
     5 0.329641   128.121.50.122  192.168.1.46    TCP      [TCP segment of a reassembled PDU]
     6 0.330326   128.121.50.122  192.168.1.46    HTTP     [TCP Previous segment lost] Continuation
     7 0.330467   192.168.1.46    128.121.50.122  TCP      1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042   128.121.50.122  192.168.1.46    TCP      [TCP Retransmission] [TCP segment of a re
```

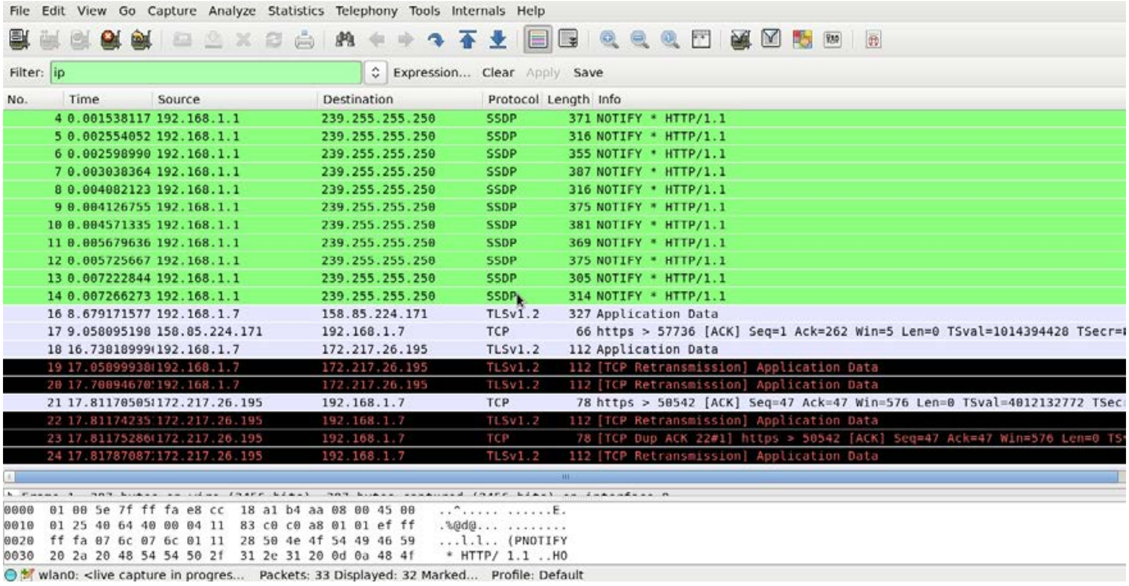
```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent:
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US;
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

File: "C:\DOCUME~1\PALLAVI~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... P: 671 D: 671 M: 0 Drops: 0

Fig. 1(b) Analyzing network packets with Wireshark

According to Fig. 1(b) one of the most important capabilities is packet capture and analysis. Being able to look into every single piece of metadata and payload that went over the wire provides very useful visibility and helps to monitor systems, debug issues, and detect anomalies and attackers. Packet capture can be ad hoc, used to debug a specific problem. In that case, only the traffic of a single application or a single server might be captured, and only for a specified period of time.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip
Expression... Clear Apply Save

```
No.  Time          Source           Destination      Protocol Length Info
   4 0.001538117   192.168.1.1      239.255.255.250  SSDP      371 NOTIFY * HTTP/1.1
   5 0.002554052   192.168.1.1      239.255.255.250  SSDP      316 NOTIFY * HTTP/1.1
   6 0.002598990   192.168.1.1      239.255.255.250  SSDP      355 NOTIFY * HTTP/1.1
   7 0.003038364   192.168.1.1      239.255.255.250  SSDP      387 NOTIFY * HTTP/1.1
   8 0.004082123   192.168.1.1      239.255.255.250  SSDP      316 NOTIFY * HTTP/1.1
   9 0.004126755   192.168.1.1      239.255.255.250  SSDP      375 NOTIFY * HTTP/1.1
  10 0.004571335   192.168.1.1      239.255.255.250  SSDP      381 NOTIFY * HTTP/1.1
  11 0.005679636   192.168.1.1      239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
  12 0.005725667   192.168.1.1      239.255.255.250  SSDP      375 NOTIFY * HTTP/1.1
  13 0.007222844   192.168.1.1      239.255.255.250  SSDP      305 NOTIFY * HTTP/1.1
  14 0.007266273   192.168.1.1      239.255.255.250  SSDP      314 NOTIFY * HTTP/1.1
  16 8.679171577   192.168.1.7      158.85.224.171   TLSv1.2   327 Application Data
  17 9.058095198   158.85.224.171   192.168.1.7      TCP        66 https > 57736 [ACK] Seq=1 Ack=262 Win=5 Len=0 TSval=1014394428 TSecr=
  18 16.73018999  192.168.1.7      172.217.26.195   TLSv1.2   112 Application Data
  19 17.05899938  192.168.1.7      172.217.26.195   TLSv1.2   112 [TCP Retransmission] Application Data
  20 17.70094670  192.168.1.7      172.217.26.195   TLSv1.2   112 [TCP Retransmission] Application Data
  21 17.81170505  172.217.26.195   192.168.1.7      TCP        78 https > 50542 [ACK] Seq=47 Ack=47 Win=576 Len=0 TSval=4012132772 TSec
  22 17.81174235  172.217.26.195   192.168.1.7      TLSv1.2   112 [TCP Retransmission] Application Data
  23 17.81175286  172.217.26.195   192.168.1.7      TCP        78 [TCP Dup ACK 22#1] https > 50542 [ACK] Seq=47 Ack=47 Win=576 Len=0 TS
  24 17.81787087  172.217.26.195   192.168.1.7      TLSv1.2   112 [TCP Retransmission] Application Data
```

```
0000  01 00 5e 7f ff fa e8 cc  18 a1 b4 aa 08 00 45 00   ..^..... ......E.
0010  01 25 40 64 40 00 04 11  83 c0 c0 a8 01 01 ef ff   .%@d@... ........
0020  ff fa 07 6c 07 6c 01 11  28 50 4e 4f 54 49 46 59   ...l.l.. (PNOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 20 0d 0a 48 4f    * HTTP/ 1.1 ..HO
```

wlan0: <live capture in progres... Packets: 33 Displayed: 32 Marked... Profile: Default

Fig. 1(c) Malicious sniffing systems detection platform

It captures only the packets sent to the host. Since many basic services, such as FTP and SMTP, send passwords and data in clear text in the packets, Sniffers can be used by hackers to capture passwords and confidential data. Fig. 1(c) describes these methods are usually enough to diagnose simple problems, but are clearly inadequate when dealing with complex network problems. This is where a high-quality network analyzer comes into play. Real-time network card utilization is a very handy 'visual tool' as it shows the bandwidth utilization of the network card used to capture packets. As a network packet analyzer, Wireshark can peer inside the network and examine the details of traffic at a variety of levels, ranging from connection-level information to the bits comprising a single packet. This flexibility and depth of inspection allows the valuable tool to analyze security events and troubleshoot network security device issues.

C. Network Security Based on Cloud Computing

Intra-cloud communication is secured from outside threats; there are still prevailing security risks due to the following:

- The transferred business data between two services could potentially be „visible" to the cloud provider.
- It is possible for a malicious neighbor instance within the same physical machine or LAN to snip the transferred business data.
- A secure cloud computing environment depends on identifying security solutions. A deeper study on current security approaches to deal with different security issues related to the cloud should be the focused of future work.
- Ensuring data confidentiality and integrity of the organizations data in transit to and from the public cloud provider.

7. CONCLUSION

The major goal of this article is to examine the role of cloud computing, and the capacity building technology of centralized computing. We looked at the framework of client-server disruption network and discussed the CB technology of client-server disruption network over cloud that brought it to the present day. CB technologies and architectural models are discussed, as well as some of the more secure cloud server offerings. The relevant network aspects are presented and discussed in detail, using wire shark for bottleneck Analysis of Traffic Monitoring.. The client-side of the proposed solution is very important as well as automatically provisions their own computing resources as needed and without requiring human intervention, typically through an interactive portal that enables them to accesses these services themselves. Architecture components, interfaces, functional and non-functional requirements of client-side have been examined to provide the reader with interesting implementation guidelines. A prototype implementation of the client-side has been described in some detail. A novel real-time simulator (real-time three-personal computer system) developed is very cost effective. The results of proposed centralized control model are compared with the conventional centralized control model.

Experimental results and security analysis demonstrate that effective data transfer between secret files is achieved while preserving their privacy.

In this paper, we developed a realistic model to quantify the boost network performance of clients and the overall provisioning cost incurred by coordinating the in-network storage capability. Based on this model, we derived the optimal strategy for optimizing the network performance and cost estimate, and evaluated the optimal strategy using real network topologies.

Our work differs from these studies in two ways. First, our network model for centric networks is unique, where we formulate the problem by focusing on the overall network performance and cost from the network carriers' perspectives. Thus, our model considers the routing performance and the coordination cost, and investigates the trade-offs between them. Secondly, by decoupling the coordinated vs non-coordinated caching strategies, the content placement is simplified and only performed for coordinated caching part. Thus, a nice property, total unimodularity holds, which allows algorithm to find the provably optimal solution.

8. REFERENCES

[1] Amitesh Singh Rajput, Balasubramanian Raman, "color me, store me, know me not: supporting image color transfer and storage in encrypted domain over cloud". IEEE International Conference on Multimedia and Expo Workshops (ICMEW), 978-1-5386-0560-8/17,2017.

[2] Jose Moura, David Hutchison, Review and Analysis of Networking Challenges in Cloud Computing. Academic Press Ltd. London, UK, ISSN: 1084-8045, pp 113-129, 2016.

[3] Fabio Baroncelli, Barbara Martini, Piero Castoldi, Network virtualization for cloud computing, Annals of telecommunications, Volume 65, Issue 11–12, pp 713–721, 2010.

[4] Zhao Jianguang, Liu Jianchen, Fan Jingjing, Di Juxing, The Security Research of Network Access Control System, IEEE Xplore, ISBN: 978-1-4244-9595-5, April 2011.

[5] Brenda Huettner, Digital Risk Management: Protecting Your Privacy, Improving Security, and Preparing for Emergencies, ISBN: 0-7803-9777-0, 23-25 Oct. 2006.

[6] Soumitra Sasmal, Indrajit Pan, Mutual Auditing Framework for Service Level Security Auditing in Cloud, IEEE Xplore 978-1-5386-1931, 2017.

[7] Haroon Shakirat Oluwatosin, Client-Server Model, OSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16,Issue 1,Ver. IX , PP 67-71. Feb. 2014.

[8] Terlochan Singh Bhatti, Nikhil Pathak, Nasiruddin, Ibraheem, "A More Realistic Model of Centralized Automatic Generation Control in Real-time Environment".Electrical power component and circuits, Taylor and francis,pp 2205-2213.sep 2015.

[9] Sandip Roy, Santanu Chatterjee, Ashok Kumar Das, On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services, IEEE Digital Object Identifier 10.1109/ACCESS.2017.2764913. September 2017.

[10] Yunchuan Sun, Yongping Xiong, Junsheng Zhang, "Data Security and Privacy in Cloud Computing",International journal of distributed sensor networks, pp:1-9, July 2014.

[11] Ravish Saggar, Shubhra Saggar, Nidhi Khurana, Cloud Computing: Designing different System Architecture Depending On Real-World Examples,International Journal of Computer Science and Information Technologies, Vol. 5 (4), pp5025-5029 2014.

[12] Jianping Zhang, Hongmin Li, Research and Implementation of a Data Backup and Recovery System for Important Business Areas, IEEE Xplore, sep2017.

[13] Pelin Angin, Bharat Bhargava, Zhongjun Jin, A Self-Cloning Agents Based Model for High-Performance Mobile-Cloud Computing, IEEE Xplore, Aug2015.

[14] Umar Mukhtar Ismail, Shareeful Islam, Haralambos Mouratidis, Cloud Security Audit for Migration and Continuous Monitoring, IEEE/Trustcom, Dec 2015.

[15] Ch. Anilkumar, R.V.Krishnaiah, "A Novel approach for unique Data Backup in Cloud Storage", International Journal of Information Technology Infrastructure. ISSN 2320 2629, PP: 1-4.

[16] Nasir Raza, "Challenges to network forensics in cloud computing, Information Assurance and Cyber Security (CIACS), IEE Conference on information assurance and cyber security. ISBN: 978-1-4673-7914-4, Dec 2015.

[17] Weili Huang, Jian Yang, New Network Security Based on Cloud Computing, Education Technology and Computer Science (ETCS), Second International Workshop on education technology and computer science. ISBN: 978-1-4244-6389-3, 2010.

[18] Revathy Nair, Amit SanWariya, Savita Shiwani, Determining best practices for windows server deployment in the cloud, IEEE International conference on advances in computing, communication & Automation, April 2016.

[19] Yanhua Li, Haiyong Xie, Yonggang Wen, Chi-Yin Chow, Zhi-Li Zhang, How Much to Coordinate? Optimizing In-Network Caching in Content-Centric Networks, IEEE Transactions on network and service management, vol. 12, Issue no.3, September 2015.

[20] Mr. Vikas Malik, Srishti Gupta, Jyoti Kaushik, Network Security: Security in Cloud Computing, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 1, pp. 3643-3651 Jan 2014.