Journal of Advancement in Computing (JAC)

A VIRTUAL DATA CENTER COMPARISON OF DIFFERENT FIREWALLS' PERFORMANCE

Hanane Aznaoui, Canan Batur Şahin
[1] #Department of computing Cadi Ayyad University, Marrakech, Morocco
[2]#Department of Computer Engineering, Siirt University, Siirt, Turkey
Email: canan.batur@ozal.edu.tr, o.b.dinler@siirt.edu.tr

ABSTRACT

Whether virtual or real, every data centre depends on its network, and the firewall is a crucial component of that network for secure communication. Different types of firewalls, such as software firewalls, physical firewalls, virtual appliance firewalls, and kernel-integrated firewalls, can secure data centre connections. When choosing a firewall, there are many things to take into account, especially in a virtualized data centre where each firewall behaves differently depending on the situation. Reduced costs, effective administration extensibility, greater resource usage, scalability, and energy resilience are just a few benefits that virtualized data centres are supposed to produce. In this study, the use of firewalls is examined in relation to virtualized data centres. The effectiveness of several kinds of firewalls, including virtual firewalls, physical firewalls, and software .The performance of various types of firewalls, such as software firewalls, physical firewalls, virtual appliance firewalls, and kernel-integrated firewalls, is being analysed. Virtual data centre firewall implementation and performance comparisons explain how to design and which firewall type provides the best performance. In all conditions, it was shown that kernel-integrated firewalls worked properly. Virtual machine IP addresses and networks can vary, and the kernel-based firewall can dynamically update its rules to keep pace with such changes.

ARTICLE INFO

Article History:
Received 5/9/2022
Revised 16/10/202
Accepted 17/7/2023
Available,Online 18/04/2023

Keywor
Firewall
Virtual machine
Data centE
Communication
Connection

1.INTRODUCTION

Controlling the flow of network data is the primary function of a packet filtering firewall. Each packet, which contains user data and control information, is examined by the firewall and tested according to a set of pre-established criteria. Packet filtering firewalls play a significant role in ensuring the integrity and authenticity of network data. It is important to consider the benefits and drawbacks of each choice before making a final decision. Filtering firewalls are classified as either No State Packet Filtering (NSPF) or Stateful Packet Filtering (SPF). There is no State Packet filtering: As long as the firewall's rules are met, it either accepts (Allow) or refuses (Deny) a packet

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

based on its header information (Deny). The stateless firewall does not keep track of TCP connection status [1-2].

In order to enable full packet filtration, select the option. A state-full firewall also monitors TCP connection status. Several flags and header fields in the TCP protocol are used to keep track of its current status, as demonstrated clearly in the research. The firewall monitors the traffic flow from beginning to end, and each packet's information is examined and kept in the status table. This is done by comparing the TCP session information in each packet to the firewall's state database and allowing or rejecting a packet based on the information. Processor, memory, and interface are physical components of physical firewalls [3].Distributed Firewall Monitors and filters virtual machine virtual NIC traffic at both the kernel and virtual NIC levels with the KIF module. A distributed firewall across multiple hypervisors can be implemented with it [4].

A virtual firewall is an additional option for implementing a firewall in a virtualized datacenter. On the hypervisor, the virtual appliance firewall is installed and monitors all communication between virtual machines. Using a pre-configured virtual appliance firewall is a straightforward process. To get started, all that is required is the loading of a virtual appliance into the hypervisor and some basic configuration. Firewall monitors for your own safety and the safety of others. A bespoke operating system runs on virtual hardware and serves the same purposes as a real firewall in a virtual appliance [5].The only difference between a virtual appliance firewall and a physical firewall is the hardware. While a physical firewall is composed of physical components such a motherboard, CPU, memory, and network interface cards, a virtual firewall is constructed entirely of software. In spite of this, most of the tasks and functionalities are the same [6].

On the VM, an if/firewall can be installed as an application. This firewall analyses traffic after being installed as software on the operating system. It is also possible to keep track of the VMs' traffic on the OS itself. A physical firewall device can be used in a virtualized data Center to monitor and safeguard virtual machine connections, providing virtual machine protection. It is necessary to have a firewall in place in order to keep track of virtual machine traffic when it connects with a physical computer network. The physical firewall in a virtualized data centre has a number of restrictions and is unable to keep track of all types of virtual machine traffic. Virtual computers connected to the same virtual switch cannot be monitored by the physical firewall (PF) [7]. The physical firewall is unable to keep track of the activities of a virtual machine when it connects to other virtual machines running on different hypervisors over the same IP network. Since the physical firewall only supports IP-based policies, it won't recognise a virtual machine's new IP address or migrate to a different IP subnet, necessitating the administrator's updating the firewall policies [8].

Distributed firewalls that analyze virtual machine traffic at both the kernel and virtual NIC (VNIC) levels are made available by the VMware NSX service. As a result, firewall rule enforcement can be scaled up without putting a strain on physical equipment. As a result, the firewall consumes only a small amount of CPU and can run at full speed. Virtual NIC cards are used to monitor and filter the traffic flowing between computers when they are connected via a network. Virtual machine traffic can be filtered using L2-L4 rules on a hypervisor's kernel-integrated firewall (KIF).

Virtual machine traffic is monitored as the hypervisor loads and begins initialization. You have the option of monitoring or excluding the traffic of all virtual machines. One of the firewall's options is a choice between two types of filters. With just a single administration panel, NSX firewall configurations are incredibly easy to manage. Using its control plane, the central administrative console sends rules and policies to the hypervisors. Every hypervisor analyzes virtual machine traffic according to these criteria, which makes it easier to monitor virtual machines across all hypervisors [9].

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

Virtual machines' traffic is tracked as it passes through hypervisors .It is possible for a distributed firewall to keep track of traffic flowing between virtual machines on the same virtual switch, as well as between virtual machines running on different hypervisors and the internet [10].

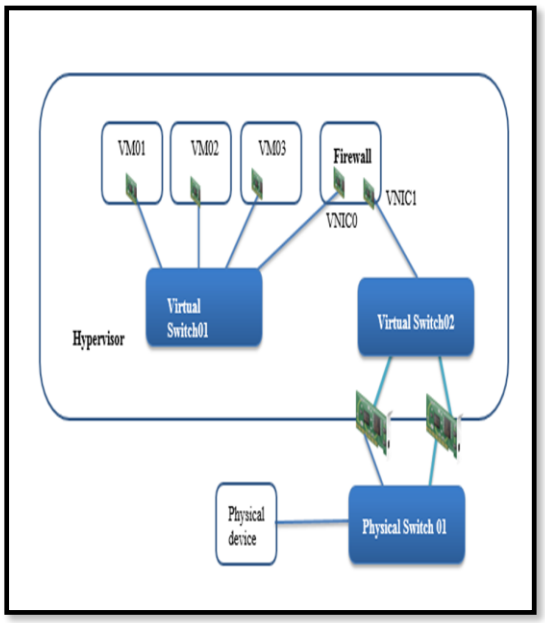

Fig 1. Firewall Virtual Appliance

A virtual firewall is another type of firewall implementation in a virtualized datacenter. All traffic from all virtual machines is monitored by a virtual appliance firewall that is deployed on the hypervisor [11].

2.RECENT WORK

ICMP queries are sent from the physical computer to the virtual machine and from the virtual machine to the virtual machine in all the study scenarios, and the throughput of the various firewalls is measured by the amount of FTP traffic. At least 10 ICMP packets are utilized to assess performance in this study (This following process is repeated 10 times to get the average result). Typical, and worst-case ICMP response times are recorded. The standard size of a packet transmitted from a source to a destination is 10000 bytes. Every time 10 packets are transmitted, the elapsed time between them is measured. Pinging a virtual machine from a real computer revealed that both machines were able to communicate via the firewall. It took 10 iterations of sending out ICMP packets and downloading 1.23 GB of data from an FTP server to the physical system [12].

It is possible to ping a virtual machine from a physical one, and vice versa, using the virtual appliance firewall to facilitate machine-to-machine communication. Ten sets of ten ICMP packets were generated, and a 1.23 GB file was downloaded from an FTP server to the physical system.

Traffic from a physical host to a virtual machine is generated and monitored using a distributed and kernel-integrated (VMware NSX) virtual appliance firewall.

Using the kernel-integrated firewall, we can ping a VM from a host computer and have the VM connect with the host over the firewall. Create ten ICMP packets and get the 1.23 GB file from the FTP server.

Virtual machines housed on two distinct hypervisors can ping one another and connect with the outside world by way of the physical firewall used in conjunction with the application firewall. The 1.23 GB file was downloaded after 10 rounds of generating 10 ICMP packets [13].

When two virtual machines are communicating behind a physical firewall, the distributed and kernel-integrated (VMware NSX) solution is utilized to produce identical traffic from one virtual machine to another while keeping tabs on it.

Use ping from one virtual machine to another and the firewall built into the kernel of each virtual machine to connect with the other virtual machines. The 1.23 GB file was downloaded from the FTP server and sent to the virtual machine after 10 ICMP packets were created [14].

Pinging a virtual machine from another virtual machine is possible when using a virtual appliance firewall, and "PfSense" is a software firewall that allows communication between virtual machines. Dependent variable, virtual datacenter, independent variables, virtual computer, real machine, physical Internet, ICMP, FTP, and Ping are all crucial parts of this study's

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

research variables. Discussion on the measuring instruments is given as.Virtual data centers provide businesses with a set of cloud infrastructure components including servers, storage clusters, and networking hardware. Using Virtual Data Center, customers may save their data on the cloud. In the virtualization hub, users may log in from any gadget. It's been estimated that [15].

A virtual machine (VM) is a type of computing resource that simulates a computer in software rather than an actual computer. Multiple "guest" computers share a single "host" computer .A VM is a software simulation of a real computer. The software that makes up a virtual machine has to be maintained in the form of updates and system monitoring in order to execute applications, operating systems, and other computer activities. Multiple virtual machines (VMs) can be hosted and operated on a single physical computer (usually a server).

While a physical/real machine is a dedicated platform for a single tenant, a hypervisor (host) may handle several virtual servers, so enabling numerous programs to operate in parallel while sharing the same set of physical resources. If you virtualize your servers, you may operate your terminal server, database server, and file server all from the same physical hypervisor [16].

Routers, cables, antennas, internet exchange points, and data centers are all examples of the physical components that make up the Internet and make it possible for us to communicate with one another. Submarine cables, which transmit telecommunication signals across oceans and seas, internet exchange points, which allow different service providers to exchange internet traffic, and data centers are all depicted in the visualization to demonstrate their physical structure and real quantity [17].

The Internet Control Message Protocol (ICMP) is a protocol used at the network level. Latency between two sites on a network may be measured using the ubiquitous ICMP protocol, which also serves to relay information about network connection difficulties back to the compromised transmission's point of origin. Destination network inaccessible, source route failure, and source quench are some of the control messages that can be sent. Information is transmitted using a packet format with an 8-byte header and a body of varying size. A device, such as a router, can utilize ICMP to notify the data packet's originator of any problems with the transmission. If a datagram fails to reach its destination, for instance, ICMP can notify the host of the failure and provide further information that may provide light on the cause of the transmission failure. It's a method of conducting business that promotes open dialogue among employees [18]. Every end user in a data center is at risk of cyberattacks. Even if the data is well-processed, there are a number of risks because most VMs are located on the same virtual server. For centuries, people have relied on traditional materials and methods to construct their homes' fire walls and other essentials. It is impossible to identify an attack on audio and video equipment that comes into contact with traditional fire barriers and other products like those. However, a hardware firewall cannot be replaced by many fireplaces, and you must just be visible between two machines in order to use their traffic monitoring features. Physical items that interfere with virtual machine migration are another problem [19].In all data centers, a firewall is a must for users, according to many examples. Consider the implications of this statement. As an IT security manager, he failed to see any internal threats to the data center, which provides all of the important services .The configuration of a firewall is more important than the configuration of other computer systems. " However, many people are afraid of putting up a firewall or data center for two reasons. Unit testing is one example of a performance.Currently, most firewalls are still in development and are designed for older systems, but they nevertheless provide the necessary protection and security features. Most firefighting realtors still design bank operational settings that have an unknown variable of what the firewall should be in the data center if this sort of firewall is positioned in a location that cannot support such a load.

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

Data centers require a firewall for numerous reasons, as stated in this article. Media management is critical in data centers, where the firewall must be implemented in a variety of physical, embedded, and virtual modes of implementation [20-21].

3. RESULTS AND DISCUSSION

Ping, ICMP delay, FTP, VM, RM, and latency are all examples of performance parameters, with throughput serving as a benchmark for determining a network's upper limit. packets received by one node at a given time is referred to as "unit time". The Ping is a network management software diagnostic utility that is used to determine whether a host is accessible on a network. Ping is a component of the Internet Control Message Protocol (ICMP) family. A timestamp is included in each packet sent by Ping, and this can be used to calculate the time it takes for a packet to travel to the remote host. ICMP is a network-layer Internet protocol that sends error messages and other information about packet processing back to the source, and this is referred to as the latency of a packet. The ICMP delay is the time it takes for a packet to get from the sender to the receiver. There are a number of significant messages generated by ICMPs, such as "Destination Unreachable," "Echo Request and Reply," "Time Exceeded," and "Timestamp Request and Reply." PfSense is a firewall/router computer software distribution based on FreeBSD that may be installed on a physical or virtual machine to create a dedicated firewall/router for a network. Web-based management means no knowledge of the underlying FreeBSD system is required to configure and upgrade it. In order to avoid being mapped by malicious networks, network managers frequently disable ICMP on network equipment. (e.g., Nmap and Nessus scans). A wide range of malicious activities, including but not limited to: ping sweeps, ping flooding, ICMP tunneling, and ICMP redirects, can all be carried out using the enabled ICMP protocol. As a "quick fix" security precaution, network managers occasionally disable ICMP traffic on their firewalls due to all of the possible ICMP assaults and the fact that TCP/IP still "mostly" works when ICMP traffic is disabled. Network security and performance may be negatively impacted by the removal of the ICMP protocol from the operating system When the ICMP protocol is restricted, it disables critical mechanisms. Tests for ICMP communication latency can uncover network connectivity and security issues. In order to get accurate findings, pfSense software uses ICMP communication delays to perform the lab setup.

The machines under test are Inspur 3060 servers, each of them contains a 8-core Dell Power Edge, R320 32 GB DDR3 RAM, 2.6 GHz Processor (8 Cores), 500 GB HDD, 4.1Gbps NIC and 7th Generation HP 380, 2.6GHz Processor, 32 GB DDR3 RAM (8 Cores), 4 1Gbps NICs 1 TB HDD, one serving a real machine and the other as a virtual machine. All of them are connected to a test intranet, with Firewall specification as: Physical CISCO ASA 5505, Virtual Appliance CISCO ASA 1000v, Integrated & Distributed VMWare NSX, and with Application PFSense. Our experiment is controlled computer, with Operating Systems & Hypervisors as: VMWare Hypervisor ESXi Version 6.0 Windows OS Server 2012, Windows 7,10. In the lab setup complete virtualized networking setup was designed where Ping from a virtual computer to a real machine in this circumstance can be generated, and these devices were intended to enable obtaining information over the physical Internet easier. 10 ICMP packets generated, ten times each, and then sent them as a 1.23 GB file to the Physical Machine through FTP. Delay has been measured on pfSense software which is an open source firewall evaluation software and firewall in itself as well [22].

4. RESULTS AND DISCUSSIONS

The findings are based on a 10x ICMP communication delay with a packet size of 10,000 bytes between the physical machine (Source) and the virtual machine. (Destination). Each time the 10 ICMP

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

packets are transmitted, the delays are investigated. The graphs are created using MS Excel; the x axis represents the time of the message according to the order in which it was sent, and the y axis represents the delay in receiving time, which is measured in milliseconds. The delays between a physical system and a virtual machine using ICMP (Internet Controlled Messaging Protocol) without a firewall are as follows and are displayed in Figure 1.

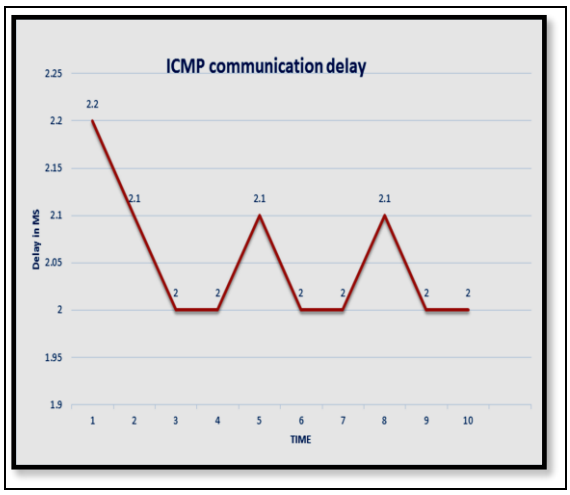

Fig .1 ICMP Delays Between a RM and a VM Without Firewall

Figure 1 illustrates the result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine without firewall measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 1.9-2.25ms with the increment of 0.05ms each time. And the latency looks very similar at delay on 2ms and the number of time intervals at 3, 4, 6, 7, 9, and 10. And again at 2.1ms on the number of time intervals at 2, 5, and 8. Latency steadily increases only on interval 1 at 2.2ms.

Physical Firewall Results

ICMP (Internet Controlled Messaging Protocol) Physical Firewall delays between physical machines and virtual machines are seen below in figure 2.These figures depict loading on physical FWs

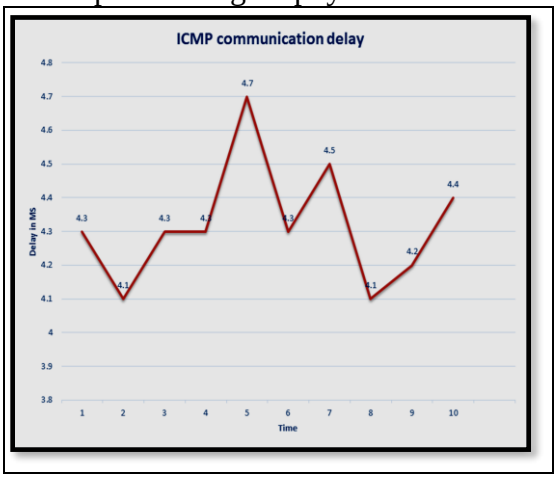

Fig.1 ICMP delays between a RM and VM with Physical Firewall through Light Load

Figure 2 illustrates the result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine with physical firewall and light load measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 13.8- 4.8ms with the increment of 0.02ms each time. And the latency looks very similar at delay on 4.3 ms and the number of time intervals at 1,3, 4, and 6. And again at 4.1ms on the number of time intervals at 2, and 8. It changes at delay 4.5 ms and the number of intervals is 7, and 4.4 ms at the interval of 10 Latency steadily increases only on interval 5 at 4.7ms. The result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine with physical firewall and full load measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 7.4-8.8ms with the increment of 0.02ms each time. And the latency looks very similar at

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

delay on 8.2ms and the number of time intervals at 5 and 10. And again at 8.4ms on the number of time intervals at 4, and 8 and 8.5ms on the number of time intervals at 1, and 9. It changes at delay 8.1ms and the number of interval is 2, and 7.9ms at the interval of 6, 8.3ms at the interval of 7 Latency steadily increases only on interval 3 at 8.6ms.

5.CONCLUSION

As part of my research, I investigated how well various types of firewalls worked in a virtualized data center. To monitor traffic as it moves through a virtual machine, it must be installed at the kernel level. In all conditions, it was shown that kernels with firewalls grafted into them worked properly. Even if multiple virtual machines are connected to the same virtual switch, the switch can nevertheless monitor and filter traffic on each of them separately. The traffic is filtered out in this circumstance other firewalls, such as physical firewalls, virtual appliance firewalls, and application firewalls, use IP-based policies and are unable to detect and update their policies if a virtual machine's IP or network changes. To ensure continual virtual machine connectivity, network managers must alter their current policy. Virtual machine IP addresses and networks can vary, and the kernel-based firewall can dynamically update its rules to keep pace with such changes. With its distributed firewall functionality, virtual machines can travel across hypervisors with no disruption to their security settings, if their policies remain the same on all of them. A kernel-based, distributed firewall is the best way to protect against viruses.

REFERENCE

[1] Haapala, H., Nurkka, P., Kaustell, K., Mattila, T., & Suutarinen, J. (2006). Usability as a challenge in agricultural engineering. Suomen Maataloustieteellisen Seuran Tiedote 21, 1–7.

[2] Goyal, S., Morita, P., Lewis, G. F., Yu, C., Seto, E., & Cafazzo, J. A. (2016). The systematic design of a behavioural mobile health application for the self-management of type 2 diabetes. Canadian journal of diabetes, 40(1), 95-104.

[3] Gawade, S., Raikar, K., & Chopade, S. (2017). Usability evaluation of agricultural websites. Paper presented at the 4th International Conference on "Computing for Sustainable Global Development"(INDIACom-2017), Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi, 136-141.

[4] Garcia, E., Martin, C., Garcia, A., Harrison, R., & Flood, D. (2011). Systematic analysis of mobile diabetes management applications on different platforms. Paper presented at the Symposium of the Austrian HCI and Usability Engineering Group, 7058, 379-396.

[5] Gao, C., Zhou, L., Liu, Z., Wang, H., & Bowers, B. (2017). Mobile application for diabetes self-management in China: Do they fit for older adults? International journal of medical informatics, 101, 68-74.

[6] Costopoulou, C., Ntaliani, M., & Karetsos, S. (2016). Studying mobile apps for agriculture. Journal of Mobile Computing & Application 3(6), 44-49.

[7] Alam, T., Ullah, A., & Benaida, M. (2022). Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. Journal of Ambient Intelligence and Humanized Computing, 1-14.

[8] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[9] Sebai, D., & Shah, A. U. (2022). Semantic-oriented learning-based image compression by Only-Train-Once quantized autoencoders. Signal, Image and Video Processing, 1-9.

[10] Alam, T., Ullah, A., & Benaida, M. (2022). Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. Journal of Ambient Intelligence and Humanized Computing, 1-14.

[11] Ullah, A., & Nawi, N. M. (2021). An improved in tasks allocation system for virtual machines in cloud computing using HBAC algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-14.

JAC 2023,https://doi.org/10.36755/jac.v1i1.46

[12] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[13] Bari, M. F., Boutaba, R., Esteves, R., Granville, L. Z., Podlesny, M., Rabbani, M. G., ... & Zhani, M. F. (2012). Data center network virtualization: A survey. IEEE communications surveys & tutorials, 15(2), 909-928.

[14] Beck, K. F., & Hämäläinen, J. (2022). Mapping the field of international comparative research in school social work. International Social Work, 65(2), 203-223.

[15] Beerbaum, D. O. (2021). Applying Agile Methodology to regulatory compliance projects in the financial industry: A case study research. Available at SSRN (4)26, 3834205.

[16] Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. British journal of management, 18(1), 63-77.

[17] Bodei, C., Degano, P., Galletta, L., Focardi, R., Tempesta, M., & Veronese, L. (2018). Language-independent synthesis of firewall policies. In 2018 Ieee European Symposium On Security And Privacy (Euros&P), 24th to 26th April,London,UK, (pp:1791-5587).

[18] Caiazzi, T., Scazzariello, M., Alberro, L., Ariemma, L., Castro, A., Grampin, E., & Di Battista, G. (2022). Sibyl: a Framework for Evaluating the Implementation of Routing Protocols in Fat-Trees. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium Conference, 25th to 29th April, Budapest, Hungry,(pp:217811).

[19] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[20] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[21] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[22] Sebai, D., & Shah, A. U. (2022). Semantic-oriented learning-based image compression by Only-Train-Once quantized autoencoders. Signal, Image and Video Processing, 1-9.