ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1581032021.pdf
https://doi.org/10.30534/ijatcse/2021/1591032021

Performance Optimization of network using load balancer Techniques

Waleed Khalid[1,2], Muhammad Waseem Iqbal[2], Tahir Alyas[3], Nadia Tabassum[4], Nida Anwar[5], Muhammad Asif Saleem[6]
[1]Lahore Garrison University, Pakistan, ch.waleed001@gmail.com,
[2]The Superior University, Pakistan, waseem.iqbal@superior.edu.pk
[3]Lahore Garrison University, Pakistan, tahiralyas@lgu.edu.pk,
[4]Virtual University of Pakistan, Pakistan, nadiatabassum@vu.edu.pk
[5]Virtual University of Pakistan, Pakistan, nidaanwar@vu.edu.pk
[6]Lahore Garrison University, Pakistan, asif.saleem@lgu.edu.pk

ABSTRACT

Load Balancer helps in increasing the speed of transmission of data across the web. It increases the performance of the network by reducing network traffic and increasing the responsiveness of the application. Two devices can connect and communicate data to one another thanks to a set of standardized rules. Participants on the internet or their service providers are assigned IP addresses by address registries. In certain conditions the protocol performs better by managing the throughput and connectivity.Cloud computing is a pioneer among the rising technologies in the IT world today. Even though cloud computing has been around for a few years, the globe has yet to reap the full benefits of this technology. Among the many revolutionary effects envisaged as a result of theThere have been few successes with cloud computing technology, and the rest of the goals are currently being worked on.research. Cloud Security and Performance are two of the most significant barriers to cloud computing adoption.stability. One of the variables that has an impact on cloud performance stability is load balancing.computing.

Key words: Load Balancer, EIGRP, VLAN, Firewall.

1. INTRODUCTION

Load balancing is a technique used to distribute load uniformly among multiple servers to increase networks' efficiency. Load balancing is essential in a network design because it reduces the burden of the network by distributing the load among multiple servers. It makes sure that the server in a network is not overburdened with requests [1].

Load balancing has several security threats that change with time. It happens over a network; during the network management, it becomes more viable towards the cyber-attack. However, in most instances, these algorithms help deal with the attacks. The most attack is a DDoS attack (distributed denial of service attack). In such an attack, a network can be rendered useless due to overwhelming service requests [2].

1.1. VLAN

VLANs stand for Virtual LANS, which is nothing but the logical grouping of network devices in the same broadcast domain. They can help reduce IT costs, improve network security and performance, provide easier management, and ensure network flexibility. VLANs address scalability, safety, and network management. Network architects set up VLANs to provide network segmentation. Routers between VLANs filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion.

1.2. ISSP

Information Security Policies or Enterprise Information Security Policies are used primarily on organizations, corporate companies, enterprise environments in general, public and private sector companies, government agencies, related companies, and offices. In general, information security policies can be and are used anywhere and everywhere. Information at rest and in transit must be safeguarded to secure them from any confidentiality, integrity, and availability issues [3].

Issue Specific Policies (ISSP) are independent and cover specific topics like a particular department or division and its asset and are meant for specific technologies. System-Specific Security Policies, SysSP, are used primarily on corporate companies or simply in enterprise environments. These policies are much targeted documents related to only specific systems they are designed to be addressed. Hence, each workplace system needs its Systems-specific Security Policies to define and outline how it functions, how to be configured, and how it is managed [4].

1.3. Cryptographic algorithm used in WEP:

WEP uses the RC4 encryption algorithm, which is known as a stream cipher. The Wi-Fi protected access is the security standard that helps the users in computing devices equipped with the wireless connection; the developed Wi-Fi alliance helps to provide more sophisticated data encryption using authentication techniques in comparison with the Wired Equivalent privacy, they have discrete modes for the enterprise's users used for the personal use, the method WPA-EAP, helps more stringent with 802.1X authentication with the help of Extensible Authentication Protocol (EAP), private mode WPA-PSK helps to pre-shared keys with the implementation and management in small offices. Enterprise modes allow the use of the authentication server in the temporal key integrity protocol [5].
Physical Layer Transparency: VLANs are transparent on the physical topology and medium over which the network is connected. A couple of essential items need to set up a VLAN or multiple VLANs such as Router, Switches and Client Network Interface Cards.
The steps include:

- Setting up the router
- Configuring the switches
- Connecting clients

1.4. IDS / IPS:

An intrusion prevention system (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Intrusion prevention systems are also known as intrusion detection prevention systems (IDS). Much like choosing between standard securities devices like routers and firewalls, it is essential to remember that no single security device will stop all attacks all the time. IPS and IDS work best when integrated with additional and existing security solutions [7].

1.5. Firewall:

In information security, a firewall is any device that prevents a specific type of information from moving between two networks, often the outside, known as the untrusted network (e.g., the Internet), and the inside, known as the trusted network. The firewall may be a separate computer system, a service running on an existing router or server, or a separate network containing several supporting devices. The different features of next-generation firewalls (NGFWs) combine to create unique benefits for users. NGFWs are often able to block malware before it enters a network, something that wasn't previously possible. They are also better equipped to address advanced persistent threats (APTs) because they can be integrated with threat intelligence services. NGFWs can also offer a low-cost option for companies trying to improve basic device security through the use of application awareness, inspection services, protection systems and awareness tools [6].

1.6. Security Issues and Attacks on the Routing Protocol

The details for handling the network of sensors that are designed for handling the energy limits, as well as focusing on data reporting to the sink nodes, are included in this LEACH protocol. As a result, the entire arrangement is based on the advertisement options, which include clustering and other broadcasting schedules. Malicious nodes that need to announce themselves as CH (Cluster heads) with a focus on the forms of the broadcast in the advertisement message tend to cause LEACH security vulnerabilities in various phases.

1.7. Auto Scaling and Flexible Load Balancing

Flexible load balancing (FLB) works similarly to a standard system load balancer, redistributing Traffic between multiple employees (EC2 occurrences for our situation). When we have to use FLB, it's a good idea to do so, Parity load across a number of EC2 instances in one or more separate Availability Zones. Use more than one EC2 instance behind the FLB and execute the same job to get a highly accessible framework. Even if one event doesn't work out, the framework will still be available. It make things simple for clients by creating a single point of contact that is maintained the same regardless of what's going on behind the heap balancer [8].

Auto scaling aids in achieving the best benefits of cloud computing. This administration automates the process of scaling up or down. When the heap normal spikes over an edge, for example, EC2 examples can be naturally included. The following are some of the advantages of using Auto Scaling:

- The possibility of maintaining the amount of register assets on an application requirements level, resulting in a framework that is extremely accessible and inexpensive;

• Controlling the health of events and replacing unpleasant events makes the framework flaw open minded.

Server Load Balancing (SLB) utilizes a series of burden adjusting calculations to provide coordinated administrations and substance conveyance. It arranges responses to specific requests from clients via the system. Worker load balancing distributes customer traffic among workers to ensure consistent, high-quality application delivery.

1.8. Design of a wireless sensor network:

In a wireless sensor network, each node in the architecture interacts with the environment using the physical parameters controlling system or sensing. The nodes interact with one another in order to do the tasks assigned to them. Each node in the wireless network architecture is connected to the others for communication [7].

Wireless sensor network protocols:

MAC: The medium access control (MAC) is used to operate the shared channel on the shared network. The most prevalent solutions in this protocol are based on connectivity. One of the connection-based network's strategies is to broadcast data to test the channel. It is a particularly dedicated network because if the protocol appears to be busy, it is unable to transfer the message and instead waits and tyres. If the connection is busy after colliding, the nodes wait in a random order, attempting to avoid colliding. In MAC protocols, there are dozens of nodes that are not involved in receiving or transmitting packets (8).

Routing: In a wireless sensor network, this is a vital function for multi hop routing. This topic has seen a significant amount of work. The wireless sensor network's routing techniques, such as MANET and the internet, are not operating properly. Internet routing has a low rate of packet errors and is one of the most reliable wired connections. On a wireless sensor network, there exist symmetric links that are dependent on the solution between neighbors; however, this is not the case. The wireless sensor network's ad hoc fashion often discovers the neighbor. The nodes are used to create neighbor network tables, and they are required to send message rounds. Before neighbor discovery, the node tables must know their geographic location. The typical functions of the geographic forwarding system, a routing algorithm.

Wireless sensor network security: It is critical for users to safeguard the wireless sensor network by maintaining the security system in the wireless sensor network to protect the users' sensitive data. Because the nodes in the network are connected via wire, there are numerous security concerns. Users of the wireless sensor network will employ a variety of strategies to protect the network from hacker attacks once it has been implemented. The network has multiple layers, each of which must be protected from a hacker attack. The network is made up of interconnected nodes that work together to keep the network running. The sensor nodes are used to examine the physical state of the network system. Routers, nodes, and gateways are only a few of the devices connected to the wireless sensor network. These are used to ensure that the network is reliable and that it can communicate with one another [9].

Wireless sensor network threats: The wireless sensor network is vulnerable to a variety of security risks. Wireless sensor networks are being employed in various aspects of life as technology advances. The new technology is preferred by the public. As previously said, this network is used in a variety of industries to connect with one another. People will safeguard the network from various types of attacks in order to protect the data from hackers [10]. The attacks include things like

- Minor assaults
- Nodes of compromise
- Denial-of-service (DoS) attacks
- Attackers who target a certain protocol
- Attempts to impersonate others

1.9. Link layer of the security architecture:

Sensors are divided into two categories: digital sensors and analogue sensors. Analog sensors provide data in the form of a continuous or waveform. The data is then processed further by the processing unit, which turns it to a human-readable format. Digital sensors generate data in discrete or digital form directly. It immediately transfers the transformed data to the CPU for further processing. Microprocessors process data using many forms of memory. On the same circuit, the memory and input/output devices are integrated. Data is stored in random-access memory (RAM) before being sent, while the operating system of sensor nodes is stored in read-only memory (ROM).

A layered technique is utilized in this research for intra and inter-cluster communication. This algorithm takes into account networks that are similar. Fairly dispersed cluster heads, according to this article, increase network longevity. The transmission range reconfiguration was utilized by the cluster heads to balance the clusters based on the number of general nodes in the cluster and the number of cluster heads. The algorithm is capable of data aggregation. This study employs an efficient scheduling algorithm for packet forwarding, which calculates the time slot for sending packets to the nodes [11].

2. METHODOLOGY

EIGRP (Enhanced Interior Gateway Routing Technology) is a network protocol that allows routers to transport data more quickly than previous protocols. EIGRP is a descendant of IGRP (Interior Gateway Routing Protocol), and routers running either EIGRP or IGRP can communicate because the measures of one protocol may be converted into the metrics of the other.

The EIGRP has been implemented over the packet tracer, which able to manage the load balancing, the major points of EIGRP are:

- Support classless inter-domain routing and enhance the variable length subnet masking
- Enabling auto summary
- Load Balance on parallel links
- Ability to use the different authentication and passwords
- Authentication and encryption
- Md5 and SHA-2 at the same time
- Topology changes over the router
- Periodically check for the available routes
- Routing process for IPv6 and IPX.
- Backward and forward compatibility

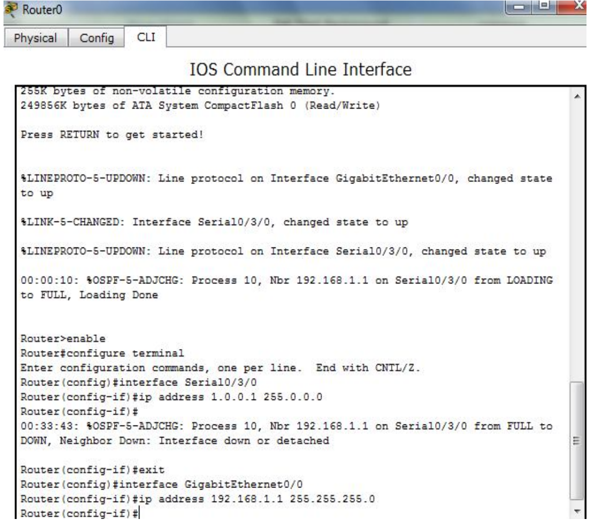
Major commands: The major commands are:

- RP/0/RP0/CPU0: router# configuration
- RP/0/RP0/CPU0: router(config)# router eigrp 100
- RP/0/RP0/CPU0: router(config-eigrp)# address-family ipv4
- RP/0/RP0/CPU0: router(config-eigrp-af)#
- hostname ROUTER-A!
- interface GigabitEthernet0/6/0/0
    - ipv4 address 10.1.1.1 255.255.255.0
- router eigrp 100
    - metric weights 0 2 0 1 0 0
    - interface GigabitEthernet0/6/0/0

The process of imagining an immensely complicated and nonlinear framework is known as great system configuration.Within that arrangement, a segment design describes how and where each component of a system is connected. It is made up of a huge number of instruments (equipment and programming) that connect the work to the system, as well as a significant number of internal connections between the various components. Each capacity of a system signifies one of the system's important capabilities.

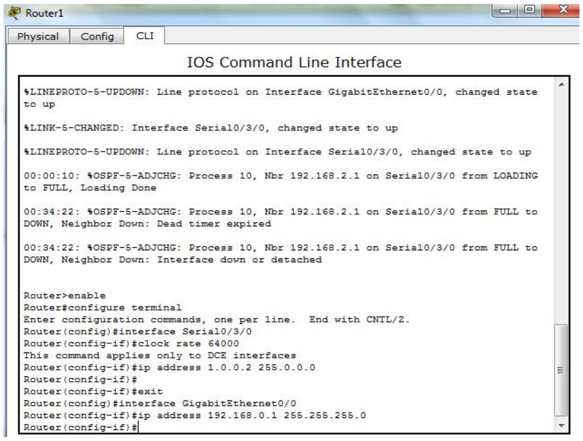
The equipment needs for system arranging and format were investigated, as well as the system structure requirements. At that point, Cisco Parcel Tracer is used to setup the equipment, which includes the switch design, IP address configuration with dynamic steering convention, and screen shots. The report also contains testing of the directing data, as required by the task. Different system administrations, such as DHCP, WEB server, DNS server, and Firewall, are considered and analyzed.

Figure 1 shows the router configuration, where the IP address was configured by using Cisco Packet Tracer. While the figure 2 shows EIGRP with load balance, testing on number of factors to evaluate the performance, the benchmark with the other protocol has been set to enhance the performance.Figure 3 shows the network testing to check the ping response with the help of Cisco Packet Tracer Command Prompt. Whereas Firewall configuration was done on the desktop to protect against the threats, this is displayed is figure 4.



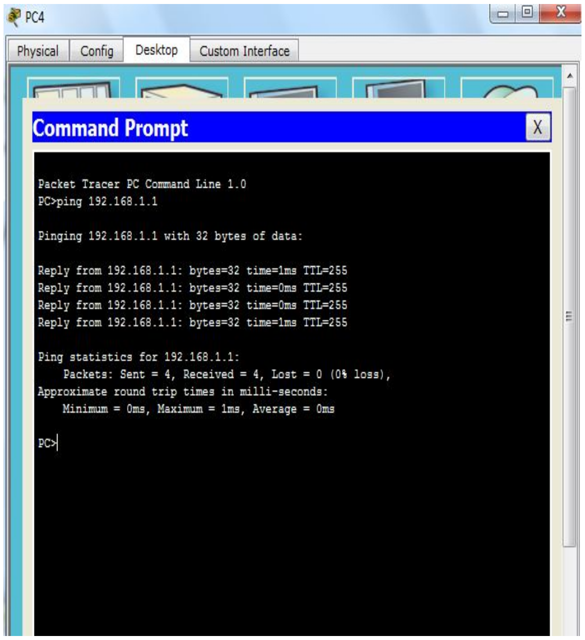
```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.1.1 on Serial0/3/0 from LOADING
to FULL, Loading Done


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/3/0
Router(config-if)#ip address 1.0.0.1 255.0.0.0
Router(config-if)#
00:33:43: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.1.1 on Serial0/3/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
```

Figure 1: Router configuration



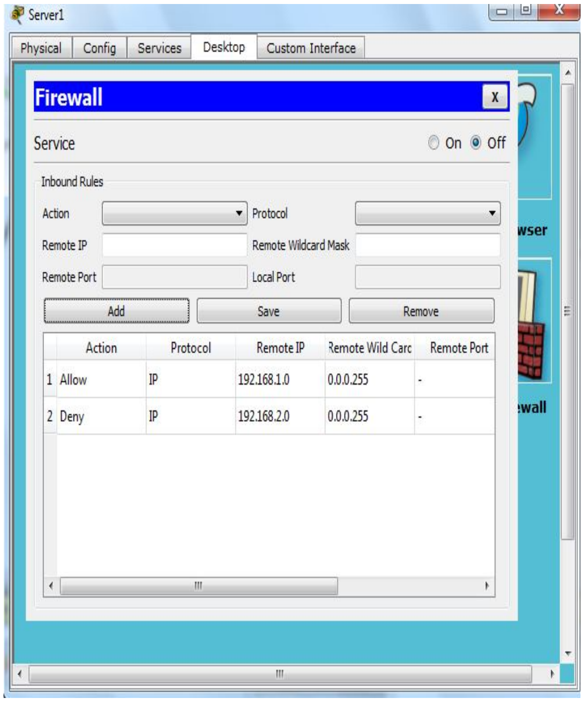
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.2.1 on Serial0/3/0 from LOADING
to FULL, Loading Done

00:34:22: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.2.1 on Serial0/3/0 from FULL to
DOWN, Neighbor Down: Dead timer expired

00:34:22: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.2.1 on Serial0/3/0 from FULL to
DOWN, Neighbor Down: Interface down or detached


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/3/0
Router(config-if)#clock rate 64000
This command applies only to DCE interfaces
Router(config-if)#ip address 1.0.0.2 255.0.0.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#
```

Figure 2: EIGRP Implementation



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Figure 3: Network test



Service ○ On ● Off

	Action	Protocol	Remote IP	Remote Wild Carc	Remote Port
1	Allow	IP	192.168.1.0	0.0.0.255	-
2	Deny	IP	192.168.2.0	0.0.0.255	-

Figure 4: Firewall configuration

3. DISCUSSION

EIGRP routers can learn about each other based on the hello protocol. Hello packets are sent from EIGRP-enabled interfaces using the router's multicast address of 224.0.0.10. A neighbor connection is established when an EIGRP router receives a hello packet from another router in the same AS (adjacency). An EIGRP and OSPF-enabled network creates an "independent system," which is not the same as a BGP-enabled network. Let's think of an EIGRP autonomous system as a collection of routers running the same protocol. "Manipulating Routing Updates," thus you should consider distributing routes among many EIGRP autonomous systems (groups).Packet transmission rates vary based on the type of medium being used. Hello packets are sent every 5 seconds on a LAN link such as Ethernet, Token Ring, or FDDI.

EIGRP topology information also includes the subnet number and mask, as well as the components of the EIGRP composite metric. Every router then computes an integer metric for each route by taking the various values for the EIGRP metric components in the EIGRP topology database and applying those values to its own configuration. The default measure calculation in EIGRP is bandwidth and latency. Cisco does not recommend including interface load and interface reliability in the computation.

OSPF, EIGRP uses three key processes to achieve the best available loop-free routes:

- First step starts with setting up EIGRP neighbor relationships (neighborships) on the same subnet with other routers.
- Step 2: This concludes EIGRP topology exchange with such neighbors. To get the current optimal route for each subnet, use the EIGRP topology data to create the current routing table.
- This three-step approach begins with the successful creation of neighbor associations between EIGRP routers. Using the network command and setting up EIGRP on your routers, as described earlier in this chapter, directs EIGRP which interfaces to use to discover neighboring routers. Once the EIGRP neighborships are established with neighboring routers, the final two steps proceed without any extra configuration.

When setting up EIGRP on a network, the network designer has the option of restricting the protocol to interfaces with no valid EIGRP neighbors. That said, by default, EIGRP requires all attached subnets to be broadcast as well. Even though R1 should never locate an EIGRP neighbor on the Fa0/0 interface, EIGRP still needs to broadcast subnet 10.1.1.0/24, which is off R1's interface. The only two alternatives an engineer has when faced with this requirement are to broadcast the subnet while also blocking EIGRP neighborships on the interface.

When you look at the configuration and regulations of EIGRP, you can see that it is nearly identical to common LAN and usual WAN technology. There are various variants, but many differences in the design and operation, particularly in the alliances formed by routers. The final section details the many configurations and designs for various VPN protocols (VPLS).

4. CONCLUSION

It should be assumed that all routers have routes to all subnets, therefore EIGRP is solely concerned with that task. It is always a good idea to first verify that the appropriate parameters have been established on each router before moving on to the next stage of design. To confirm the proper adjacencies are operational, the next step is to make sure the EIGRP adjacencies are valid. To guarantee that each subnet network has an entry in the EIGRP topology table, search for it in the EIGRP topology table. To verify all important routes are present, it is critical to thoroughly examine each router's IP routes.

REFERENCES

1. Drissi, Saadia, SihamBenhadou, and Hicham Medromi. **A new shared and comprehensive tool of cloud computing security risk assessment**, In International Symposium on Ubiquitous Networking, pp. 155-167, Springer, Singapore, 2015.
2. Arora, Vishal Kumar, Vishal Sharma, and Monika Sachdeva. **A survey on LEACH and other’s routing protocols in wireless sensor network**,Optik 127, no. 16 (2016): 6590-6600.
3. Stivala, Alex D., Johan H. Koskinen, David A. Rolls, Peng Wang, and Garry L. Robins. **Snowball sampling for estimating exponential random graph models for large networks**, Social Networks, Vol. 47, PP 167-188, 2016.
4. Boulhares, Imane, and Mohammed Omari. **Hybridizing PEGASIS with LEACH-1R protocols in wireless sensor networks**, In 2016 8th International Conference on Modelling, Identification and Control (ICMIC), pp. 1037-1042. IEEE, 2016.
5. Han, Peiyi, Chuanyi Liu, Yingfei Dong, Hezhong Pan, QiYang Song, and Binxing Fang. **FileCrypt: Transparent and scalable protection of sensitive data in browser-based cloud storage**, In 2019 IEEE Conference on Communications and Network Security (CNS), pp. 46-54, IEEE, 2019.
6. Ji, Changqing, Yu Li, WenmingQiu, UchechukwuAwada, and Keqiu Li. **Big data processing in cloud computing environments**, In 2012 12th international symposium on pervasive systems, algorithms and networks, pp. 17-23, IEEE, 2012.
7. Hill, Jason Lester. **System architecture for wireless sensor networks**, University of California, Berkeley, 2003.
8. Perillo, Mark A., and Wendi B. Heinzelman. **Wireless Sensor Network Protocols**, PP 1-35, 2005.
9. Perrig, Adrian, John Stankovic, and David Wagner. **Security in wireless sensor networks**, Communications of the ACM 47, no. 6, PP 53-57, 2004.
10. Karlof, Chris, and David Wagner. **Secure routing in wireless sensor networks: Attacks and countermeasures**, Ad hoc networks 1, no. 2-3, PP 293-315, 2003.
11. Hafiz Hasan Naqvi, Tahir Alyas, Nadia Tabassum, Umer Farooq, Abdallah Namoun and Syed Aun M. Naqvi.**Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward**, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 10, No. 3, pp. 2533 – 2539, 2021.