Enhancing the Quality of Service of Cloud Computing in Big Data using Virtual Private Network and Firewall in Dense Mode

Hussain Shah[1]
Department of Computer Science
Islamia College University,Peshawar, KP, Pakistan
Institute of Computer Science and Information Technology
University of Agriculture, Peshawar, KP, Pakistan

Aziz ud Din[2]
Shaykh Zayed Islamic Centre
University of Peshawar, Peshawar, KP, Pakistan

Abizar[3], Shams ud Din[5]
Department of Computer Science
Islamia College University, Peshawar, KP, Pakistan

Adil Khan[4]
Department of Computer Science
University of Peshawar, Peshawar, KP, Pakistan
Shaykh Zayed Islamic Centre
University of Peshawar, Peshawar, KP, Pakistan

***Abstract*—Cloud Computing entails accessing and storing programs and data over the internet instead of the hard drive of a personal computer. Over the Internet, it is the practice of software and hardware to pass a service. Cloud gives the ability to consumers to access big data and use applications from every device that can have access to the internet, however, the key problem is security and this can be solvable by a firewall and Virtual Private Network. Recently, research has been accomplished in deploying firewalls and Virtual Private Networks with parameters of throughput and load in sparse mode. In this paper, an examination of firewall and Virtual Private Network is considered based on average throughput, average packet loss and average end-to-end delay in dense mode. To examine the performance of cloud computing without Firewall and Virtual Private Network, with firewall only, and with firewall and Virtual Private Network is the research goal. The simulation results have shown that Firewall and Virtual Private Network offers better security through a wide investigation with slight distress in the cloud performance.**

***Keywords*—Cloud computing; big data; firewall; virtual private network; security; performance**

I. Introduction

The Internet is growing vigorously these days. The cost of storing data, the power consumed by computers, and the hardware are increasing and expanding. The storage space in the data centre isn't enough to meet the requirements. Also, the system and service of the internet can't solve the said issues. The researchers and academia work to find new solutions. At the same time, large enterprises have to study data sources entirely to support their business. The collection and analysis must be built on a new platform such as Cloud Computing. In [1], the need for Cloud Computing by the business community is addressed? It is stated how to utilize the resources of a computer, how to increase the economic efficiency by improving the utilization rate, and how to decrease the equipment energy consumption. Cloud Computing is a computing technique in which capable and changeable information technology (IT) gives service to external clients using internet technology. Cloud Computing is not a fundamental idea instead it's a developmental concept that combines different existing techniques to recommend a new useful IT providing tool. Through the internet, Cloud applications expand their availability and accessibility by using large data centres and powerful servers that host web applications and services [2]. Those who have a standard internet connection, as well as browser, can be connected to the cloud applications. Cloud-based computing is a model that allows suitable on-demand network access to a shared pool of configurable assets of computing resources (e.g., networks, servers, storage, services, applications) that could be quickly provisioned and released with minimal management efforts or service provider interaction [3].

Cloud Computing technique helps in computing different tasks like efficiency, reduced cost, performance, quick deployment and easy access to the information, etc. The important issue in cloud computing is the security which needs to be improved. Earlier a couple of security mechanisms such as firewall and VPN has already been introduced and standardized for guaranteeing the security that influences the cloud performance in regards to the quality of service parameters. As per the literature survey, very few research attempts have been observed and prepared to examine average end-to-end delay, average throughput and average packet loss in dense mode.

In this paper, the research is carried out on VPN and firewall in a dense mode that base on the average throughput, average end-to-end delay and average packet loss using the OPNET 14.5 simulator.

A. Applications of Cloud Computing

Cloud Computing provides several benefits to cloud users where one of the application is presented below in Fig. 1 for more observation.

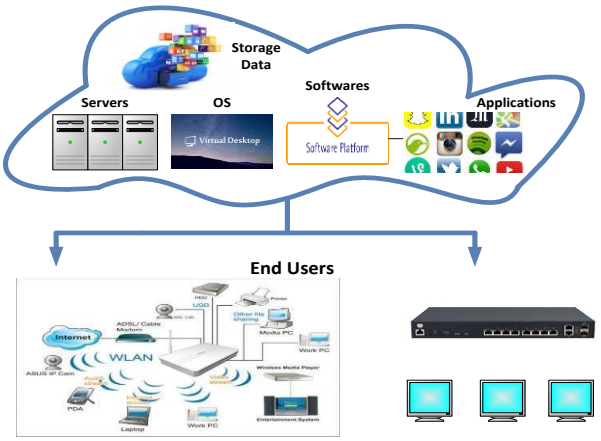

Fig. 1. A Cloud Application.

1) E-Learning: Cloud Computing is a significant technique that can be used in education (e-learning) to create attractive environments for teachers, students, and researchers to retrieve information by using the cloud of parent organization [4].

2) E-Governance: A government can provide an efficient service to its citizens, institutions, and their cooperation by using Cloud-based computing [5]. This can make the environments more scalable and customizable by reducing the energy to manage, install, and upgrade the applications.

3) Cost efficiency: By using the Cloud Computing technique, the Cost and budget of a company can be reduced to a great extent rather than relying purely on traditional desktop-software based approaches [6], such as it provides the facilities to users or customers to use hardware and software owned by other companies without the hesitant of managing and purchasing them, or without purchasing the required application by accessing the third party servers with the help of internet.

4) Almost unlimited storage: Unlike traditional desktop-based computing approaches. Cloud computing offers the facility of unlimited storage.

5) Backup and recovery: As compared to physical desktop hard drives, in cloud computing the data is stored on many servers across the globe where one can easily retrieve data from the cloud [7].

6) Easy access to information: By accessing the cloud one can easily upload and download data from anywhere in the world by using different gadgets.

7) Automatic software integration: Cloud-based computing is the automatic integration system that can integrate and update the software automatically which means that there is no need of the user to update the software itself.

8) Quick deployment: One of the vital advantages of cloud computing is its fast deployment. Once the account and procedure of data uploading and downloading are familiarized, then the user can easily retrieve data anywhere by using the application with the appropriate support of internet connection.

9) Fresh software: With the help of SaaS (Software as a Services), Cloud computing provides the latest version of software's to use in commerce and also to clients when they are released [8].

10)Always-on availability: The cloud providers are trustworthy to deliver their services and facilities to users/customers as efficiently as possible.

B. The Architecture of Cloud Computing

From the architecture perspective, the cloud computing architecture is composed of several important characteristics or components, three service models and five deployment models, that are illustrated in Fig. 2.

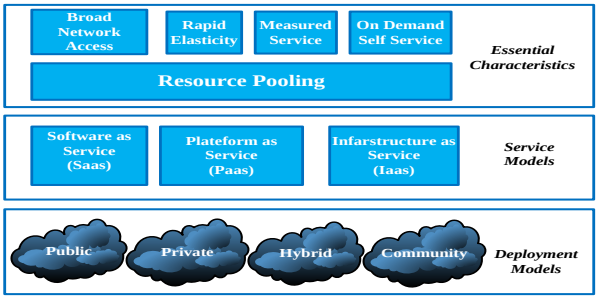

Fig. 2. The Architecture of Cloud Computing.

1) Deployment models of cloud: Cloud-based computing is established [9] on settlement models such as Public Cloud, Private Cloud and Hybrid Cloud, moreover, for different purposes, community cloud networks and mobile cloud are also used.

a) Public Cloud: This model delivers and stores a huge size of data and other facilities for the access of the general community from facility providers, spending facilities as pay/ use or cost-free.

b) Private Cloud: This model is used in fog computing by a different organization and recycled via the certified worker of that organization. In other words, Private cloud is one of the deployment models that is normally used by an individual organization or used by the authorized users of that organization.

c) Hybrid Cloud: In such systems, the organization use the important data or information on the private cloud, and the data which is less secured is being used on public could thus in such a situation the Hybrid Cloud is commonly preferred to be used, which means that this model is the mixture of double models of Cloud deployment such as community, private or public cloud models.

d) Community Cloud: A community cloud is a distinctive model of cloud deployment in which an organization is dispersed by numerous organizations that chain a precise community that has mutual concerns. A community cloud is shaped when numerous organizations share common infrastructure with similar necessities.

e) Mobile Cloud: The practice of cloud computing in mixture with portable mobile devices is known as being a Mobile cloud [10]. The occurrence of Cloud computing

happens when on the internet data and information are kept somewhat compared to separate strategies, giving access on demand. In the situation of mobile cloud, applications run on the server remotely and formerly user receives them. Mobile applications are rapidly developing a section of the worldwide mobile market. Several mobile corporations have their cloud and the user takes functionality from the mobile cloud.

2) Services model of cloud: Cloud computing service suppliers provide the three services to the end-user such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) [11].

a) Infrastructure as a Service (IaaS): Infrastructure as a Services (IaaS) provides physical components over the internet. Infrastructure as a Services provides the Infrastructure physically or virtually such as load balancer, virtual machine, data storage spaces, caching. IaaS is known as Hardware as a Service, as in IaaS the clients aren't afraid of managing and purchasing data centres and hardware's as all these things are controlled by the cloud service provider. The Cloud services provider could allow one to store data in the data center based on the size requested. A few examples of IaaS include Google drive, VMware and Rack space.

b) Software as a Service (SaaS): It permits customers to execute the available online application and software. These are retrieved over the internet. Such types of the platform in cloud computing transfer programs to millions of clients or user over the browser. SaaS is normally employed in the human resource management system and ERP (Enterprise Resource Planning). Google Applications and Zoho Office are giving such services too. Microsoft Word, Google docs, Facebook, Twitter, Gmail, and Google Calendar are some other examples of SaaS.

c) Platform as a service (PaaS): Platform as a service lets (PaaS) is a variety of cloud computing that provides a platform for the user to build and install some fresh applications online. Such as to build software or website. The main goal of PaaS is to develop, deploy and test the code effortlessly. A few examples of PaaS are Engine Yard, Force.com, Google App Engine, Apache Stratos, Azure, and Yahoo Pipes.

C. Security Issues in Cloud Computing

Cloud computing comes up with numerous major issues and trials concurrently. Like availability, performance, and security. In [12], amongst the challenges in Cloud computing, security is one of the significant and critical issues.

The security challenges in Cloud-based computing are very vast, dynamic and versatile [13]. Location transparency and data location is an important issue in the security of Cloud computing as the record is stored on virtual servers in the cloud. The users without knowing the exact location of its data storage due to which the act about data protection might be violated and affected.

In Cloud-based computing, security issues occur due to the usage of the network in Cloud computing, as users want a network connection to enter that information and resource that is of need [14]. Due to which an unauthorized user may also interfere in the network of Cloud computing. As shown in Fig. 3, the security issues are rated up to 74.4% amongst all the challenges faced by Cloud Computing.

The main issue in Cloud-based computing is to assure security. Therefore, a security technique needs to be deployed that permits only those users who are authorized and blocks those users who are not trustworthy in the cloud computing network. Two methods or techniques are deployed in an association such as firewall and VPN to improve the security in Cloud-based computing. VPN is one of the preferred technique that is used for secure data transmission from and to the Cloud. Within the VPN secured and reserved sub tunnels can be generated. VPN connects and transmits data with the help of a concept called tunneling. First, the packet is protected (encapsulated) in a fresh packet by a fresh header before it is transmitted into the VPN tunnel. The header provides information about the router of the corresponding packet, while the packet is roaming in a network that is shared before it is gotten by the tunnel destination. This encoded track is enveloped or compressed in which the packet travels is known as a tunnel. This summarized packet is 'de-capsulated' and sent to the final destination when it extends the endpoint of the tunnel. Both the termination points of the tunnel desires to provide a similar tunneling protocol. That protocol works on the data link layer (layer two) or the network layer (layer three) of the open system interconnection (OSI) model. The best well-known protocol used for VPN is Internet protocol security (IPsec) and point to point tunneling protocol (PPTP). VPNs are usually employed by using the IPsec. It is a standard way for the employment of a VPN. The IPsec and VPN are recognized very well and developed in a manner to offer strong security which gives access control, data confidentially and authentication. By assimilating IP security infrastructure into the wireless LAN's infrastructure is a simple effort to transmit wireless traffic and the VPN will provide the security to that traffic [15] as shown in Fig. 4.

A firewall is used for packet filtering between the outside world and the internal network. As the firewalls have been employed on large public networks from many years that's why firewalls have been used with VPN. Another reason for using a firewall with VPN is because of its important role and the security of the network. The joint implementation of firewall and VPN has a great impact on the performance of Cloud Computing in terms of quality of service (QoS) parameters [16].

D. Firewall

A firewall is a device used for security that detects incoming and outgoing traffic for network and a choice is made on the basis that which packet needs to be allowed and which to be blocked based on administration policy for the firewall [17]. It is like a barrier and the entire traffic (leaving or arriving) must be passed via this barrier. Only permitted traffic as defined by the cloud service provider in local security policy that will be allowed to pass. The firewall is normally considered as a tool that filters the packets, that acts as a barrier between the public and private networks. The word firewall is used in a computer that implies a device that guards the network against traffic that is untrusted.

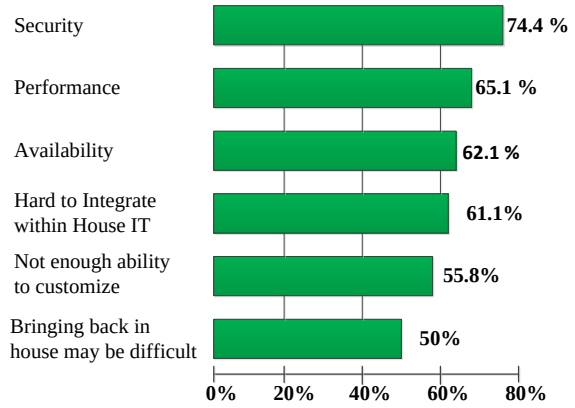

Fig. 3. Challenges to the Cloud Computing.

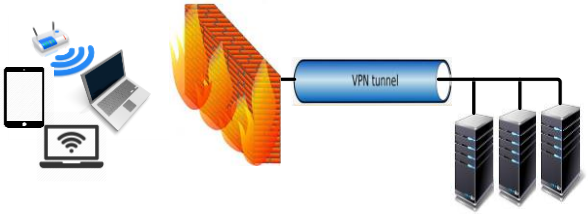

Fig. 4. VPN Procedure within IPSec.

1) Types of firewall: Firewalls are classified into three basic types: proxy servers (that is divided into two subtypes application gateways, circuit-level gateways firewall), state-full packet filters and packet filters firewall [18], as shown in Fig. 5.

a) Packet Filters Firewall: One of the most basic types of firewall is the packet filter firewall. Packet filter is applied for safety to shield the inside network users from outside network threats. This kind of firewall is the initial firewall that is used for the security of the network. It is used to monitor network entrances or access by observing incoming and outgoing packets and then making a decision based on the interior protocol address (IP address) of source and destination to allow and halt packets from the network. This packet filter firewall works on the third layer of the OSI model which deliver highly effective security mechanism. This kind of firewall is also known as static filtering. When it is implemented in a network the packet filtering is one of the most important procedures that are essential for security concern.

b) Proxy Servers: A proxy server is a kind of firewall that saves and shelters the properties of the network by data filtering at the seventh layer of the OSI model. This kind of firewall is the best kind of firewall. It provides security that is improved due to proxy data and information that doesn't allow transmitting over proxy as proxy acts as an intermediate between server and clients. A proxy server firewall provides and delivers internet access to network users. They are either on the application layer or the transport layer. This type of firewall is of two categories one is application gateway (work on application layer) and second is the circuit-level gateway (work on transport layer).

c) State-full Packet Filters: State-full packet filters are similar to a screen that exists between the server and users. This device uses state-full packet filtering for observing all packets of data when arrived on the screen. The screen examines the data based on the set of security policies.

E. Virtual Private Network (VPN)

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the internet, by allowing users to establish a virtual private "tunnel" to securely enter in internal networks, accessing resources, data and communications via an insecure network such as the internet. A VPN is a private network connection [19] that provides one's a facility of secure connection in existing public network in a remote area. In VPN each record (video, voice, and file) is an encrypted form goes to a secure virtual tunnel among the clients and the VPN provider server to cloud computing services.

1) VPN tunneling: A VPN tunnel is an encoded or encrypted or cipher path between a user and another network. To learn more that how a VPN works then it easily understand to looking at the procedure of tunneling data. A VPN tunnel is often called a virtual private network which is an encrypted path between one's computer and the server of VPN that provides the VPN services. As the connection is encrypted nobody is allowed to monitor, modify or stop one's communication. All of the communication and the data is travel in a VPN tunnel so nobody is allowing to examine the data. The VPN tunnel protects one's chatting, browsing and all other traffic from the snooping eyes of one's Internet service provider (ISP), government and also from the person who controls the Wi-Fi (wireless fidelity) which one uses to connect as shown in Fig. 6 [20].

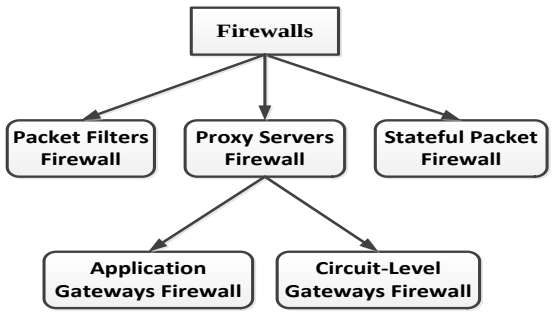

Fig. 5. Different Types of Firewalls.

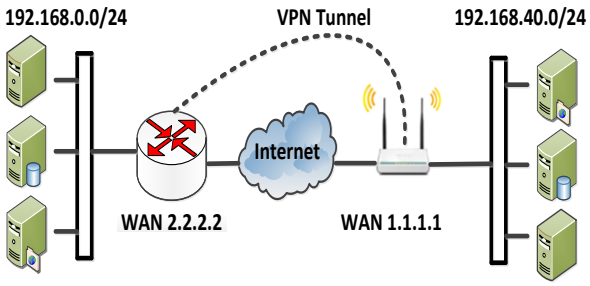

Fig. 6. VPN Tunneling.

2) Privacy in VPN tunnel: A VPN tunnel offers safe and free of intrudes connection [21]. Moreover, using VPN hides the IP address, and browsing data. Nobody can discover your real locality or IP address if one is using a VPN tunnel. One's VPN server will be merely catchable.

II. Related Work

After studying the literature in Cloud computing, different techniques are used for ensuring the security of networks, such as firewall and VPN. Firewall plays a vital role in network security because a firewall can scan all the traffic on the network and filter the packets and allow only those packets or users which are authorized. While implementing a firewall, the network administrator faces issues of conflicting policies. A firewall supports multiple distributed policy which may cause delay, system overhead and time-consuming. Various authors have used firewall and VPN for security purpose however every one has its limitations. In this paper, the issue of security is the main problem in the wireless LAN standard IEEE 802.11 in Cloud computing [22].

The performance is a major issue as the firewall tool checks all incoming and outgoing packets, it consumes time and produces overhead in the system which affects the service level agreement (SLA) [23]. A cloud-based firewall is difficult to configure efficiently. To support distributed processing environments and to overcome the conflict of making security policy rules set by the network administration [24]. Implementing Firewalls cost enough budget as for as low-level business is concerned. The amount of implementing a firewall is approximately 116,075$ for one year to keep its deployment and maintenance [25]. VPN is a security mechanism that allows user to access common applications such as HTTP, load, Email. However, using the VPN can achieve the security but it also degrades the performance of the network in terms of throughput, etc. [26]. Once some attacks occur against Cloud service the response time of system firewall becomes overhead of performance due to the huge arrival of packets. So, it will take a long response time which will be the violation of service level agreement (SLA) and the decrease in customer fulfilment [27]. In a computer networking environment, a firewall protects internal nodes from the external attack and the internal nodes as well because a firewall is managed by the system administrator. Therefore, it is needed to handle the firewall in a new way which satisfies the requirement of Cloud computing [28]. Firewalls can be an essential part to secure network that prevents hackers away from a computer network, in this regard, the procedure of configuring a firewall is a difficult and stressful job [29]. When the external users try to enter the Cloud computing network, so, first they undergo through the vital barrier of firewall that provides networks security and allow only those users who are compliant and give safety from different attacks such as HTTP DoS (Denial of service) or brute force attack.[30, 31].

III. Methodology

A. Simulation Parameter Selections

The parameters used in the simulation are given below in Table I.

TABLE. I. Parameter for Simulation

Parameters	***Description***
Simulation tool	OPNET modular 14.5
Standards	IEEE 802.11g (WLAN)
Time	5 Minutes
Area	100 m x 100 m
Nodes	18
Workstations	03
Access points	03
Servers	03
Protocols	OSPF
Applications	HTTP, FTP, Email

B. Performance Parameters

In this research there are three performance parameters used are discussed as follows.

1) Average throughput: The number of successfully received packets from source to destination as per unit time. It is calculated in bits per second (bps) or packet per second and can be calculated as shown in equation (1).

$$\text{Average Throughput} = \sum_{i=1}^{n} \frac{(\text{Received Packet i x Packet Size})}{\text{Simulation Time}} \quad (1)$$

2) Average end-to-end delay: It is the total time taken by a packet to reach from source to destination and is represented in seconds/millisecond. Thus, in the research work achieved, one of the parameters is the average end-to-end delay as declared in equation (2).

$$\text{Average End to End Delay} = \sum_{i=1}^{n} \frac{(\text{Packet Received time i - Packet Sent time i})}{\text{Total number of packets } (n)} \quad (2)$$

3) Average packet loss: Packet loss happens whenever a packet flops to the extent of the target while roaming through a network of computers. It is normally initiated by crowding over a network. In the presence of Firewall and VPN, it is also significant to investigate the average packet loss and can be calculated as stated in equation (3).

$$\text{Average Packet Loss} = \sum_{i=1}^{n} \frac{(\text{Packet Loss}_i \text{ x Packet Size})}{\text{Simulation Time}} \quad (3)$$

C. Network Objects

The following objects are used.

1) Applications Configuration
2) Profile Configuration
3) IP VPN Configuration
4) Wlan wkstn **(**clients**)**
5) ip32 cloud(Internet)
6) ethernet4 slip8_gtwy (router)
7) wireless Ethernet slip4 Router (Access Point) which configured on BSS.
8) Ethernet slip8 firewall (firewall)
9) PPP DS1
*10)*ppp server (server)

D. Network Simulation Scenario

In this paper, the optimize network simulator was chosen that contain three different scenarios that will investigate the performance of the network with different illustration as mention below.

1) Without firewall and VPN scenario: In the scenario shown in Fig. 7, there are several workstations connected to three Access Points (Access Point-1, Access Point-2, Access Point-3) which are configured for three BSS. The Access Points are connected by PPP-DS1 to IP cloud (Internet) and then further connected by PPP-DS1 to Router D connected by PPP-DS1 to three Servers (Server AA, Server BB, Server CC) which represents three departments. The scenario architecture and layout are as shown in Fig. 7.

2) With firewall no VPN scenario: In the scenario shown in Fig. 8, there are several workstations connected to three access points (Access Point 1, Access Point 2, Access Point 3) which are configured for three BSS. The access points are connected by PPP-DS1 to IP cloud (Internet), then further connected by PPP-DS1 to Firewall and Router D by PPP-DS1 to three Servers (Server AA, Server BB, Server CC) which signifies three departments. In the scenario, the firewall is selected to stop servers from any exterior entree to/ (browsing over the web) from the servers.

3) With firewall and VPN scenario: In the scenario shown in Fig. 9, several workstations are connected to three access points (Access Point 1, Access Point 2, Access Point 3) which are configured for three BSS. These access points connected by PPP-DS1 to IP cloud (Internet), then further connected by PPP-DS1 to Firewall and Router D by PPP-DS1 to three Servers (Server AA, Server BB, Server CC) which represents three departments. In the last scenario, the firewall is used to stop servers from any outside access to HTTP (web browsing). The VPN tunnel would be chosen to let the clients (PCs) from Access Point-1 to access HTTP (web browsing) from the servers in the scenario. The traffic generated by Access Point-1 is not cleaned by the firewall and let users from the Access point-1 because the IP packets in the tunnel will be condensed inside an IP datagram. The scenario design and arrangement is as shown in Fig. 9.

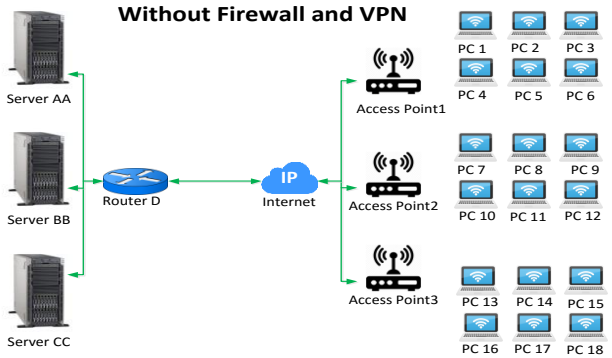

Fig. 7. The Architecture and Layout of Scenario-1.

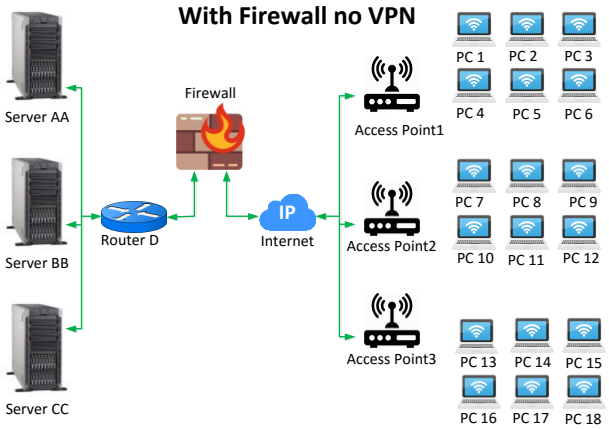

Fig. 8. The Architecture and Layout of Scenario 2.

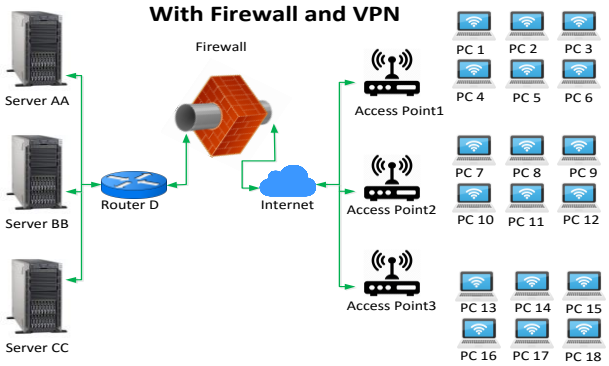

Fig. 9. The Architecture and Layout of Scenario-3.

IV. Comparison and Analysis

After implementing the scenario, the results are packed, stored and compared with each other, then the results are graphed by using the Origen Lab 2020, the parameters selected for the decision are average throughput, average end-to-end delay, and average packet loss.

Three scenarios had been prepared to examine the impact of firewall and VPN in Cloud-based computing in current research by using optimized network modular 14.5 simulators. In the paper, the results and graphs are discussed below for investigating the performance of the Cloud computing network after applying a firewall and VPN.

A. Simulation Results

For each scenario, to inspect the performance of Cloud computing "without Firewall and VPN", "with Firewall no VPN" and "with Firewall and VPN" are used, the following three performance parameters that are 'Average Throughput', 'Average End-to-end Delay', and 'Average Packet loss'.

1) Average throughput: The number of successfully received packets from source to destination as per unit time. It is calculated in bits per second (bps) or packet per second.

Table II expresses simulation results of the average throughput with no Firewall no VPN, with Firewall no VPN and with Firewall VPN in the Cloud computing network.

TABLE. II. RESULT OF AVERAGE THROUGHPUT FOR NO FIREWALL NO VPN, WITH FIREWALL NO VPN AND WITH FIREWALL AND VPN

Time	Average Throughput (bits/second)		
	No Firewall No VPN	Firewall No VPN	Firewall VPN
0	0	0	0
50	2204.44	853.33	852.30
100	1558.58	873.41	843.29
150	80887.11	66030.11	52521.20
200	6547912	50596.71	41936.02
250	56489.87	47249.27	43493.59
300	51708.13	42186.77	40323.41

Fig. 10 shows the comparison of average throughput for "no Firewall and no VPN", "with Firewall no VPN" and "with Firewall and VPN" in Cloud-based computing. 18 nodes and 3 servers are included in the scenario. The simulation time per second is displayed on the horizontal axis, whereas the network average throughput (bits/sec) is displayed on the vertical axis. The network average throughput presence of no firewall no VPN is represented by the square line while network average throughput presence of with firewall no VPN is showed by circle line, whereas the network average throughput presence of with firewall and VPN is presented by triangle line. The average throughput improved with the presence of nodes 'without firewall and VPN' as compared to 'with Firewall no VPN' and 'with the firewall with VPN' by the wide investigation since without any hurdles users can send and receive the data. The impact of 'firewall and VPN' on the cloud computing network is verified and It has been confirmed from the graph that the presence of 'no firewall no VPN' gives an improved rate of average throughput than the presence of 'firewall and no VPN' and 'with the firewall with VPN' in a cloud-based computing network. It was revealed through broad simulation that firewall and VPN affect cloud performance while provides better security.

2) Average end-to-end delay: It is the total time taken by a packet to reach from source to destination and is represented in seconds/millisecond.

Table III expresses the simulation results of average end-to-end delay with no Firewall no VPN, with Firewall no VPN and with Firewall VPN in Cloud computing network.

Fig. 11 shows the comparison of average end-to-end delay for 'no firewall and no VPN', 'with Firewall no VPN' and 'with a firewall with VPN' in Cloud-based computing. 18 nodes and 3 servers are included in the scenario as well. The simulation time per second is displayed on the horizontal axis, whereas the network average end-to-end delay (sec) is displayed on the vertical axis. The network average end-to-end delay (sec) presence of 'no firewall no VPN' is represented by the square while network average end-to-end delay (sec) presence of 'with firewall no VPN' is showed by circle line, whereas the network average end-to-end delay (sec) presence of 'with the firewall with VPN' is presented by triangle line. The average end-to-end delay slightly greater 'with no firewall and no VPN' in comparison 'with Firewall no VPN' and 'with the firewall with VPN' as all clients had willingly requested for all three applications like HTTP, FTP, Email so that's why a huge amount of traffic was accessible. Besides, in the presence of a firewall, the firewall has blocked the HTTP traffic and the only VPN give open access to its users to use this traffic. When in the network, users are limited so its Average end-to-end delay will also get reduced like results shown below in Fig. 11. The graph shows the influence of the firewall and with a VPN on a cloud-based computing network. It is proved from the results that in presence of no firewall and no VPN average end-to-end delay was slightly greater than the presence of 'firewall no VPN' and 'with the firewall with VPN' in a network of cloud-based computing.

3) Average packet loss: Packet loss happens whenever a packet flops to the extent of the target while roaming through a network of computers. It is normally initiated by crowding over a network. In the presence of Firewall and VPN, it is also significant to investigate the average packet loss.

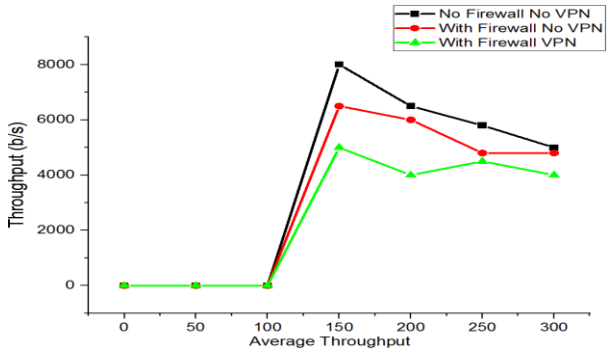

Fig. 10. Simulation Result of Average throughput for No Firewall No VPN, with Firewall No VPN and with Firewall VPN.

TABLE. III. RESULT OF AVERAGE END-TO-END DELAY FOR NO FIREWALL NO VPN, WITH FIREWALL NO VPN AND WITH FIREWALL VPN

Time	Average End-to-end Delay (second)		
	No Firewall No VPN	Firewall No VPN	Firewall VPN
0	0	0	0
50	0.00028745	0.000259	0.000259
100	0.000275809	0.000285	0.000285
150	0.000680813	0.000638	0.000621
200	0.000713229	0.000585	0.000659
250	0.000764209	0.000631	0.000712
300	0.000854009	0.000713	0.000738

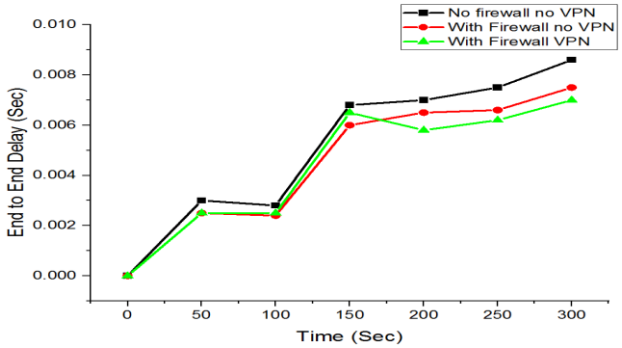

Fig. 11. Simulation Result of Average end-to-end Delay for No Firewall No VPN, with Firewall No VPN and with Firewall VPN.

Table IV represents the simulation results of average packet loss, simulation results of no Firewall no VPN, with Firewall no VPN and with Firewall VPN in the Cloud Computing network.

Fig. 12 demonstrates the comparison of average packet loss for 'no firewall no VPN', 'with Firewall no VPN' and 'with a firewall with VPN' in Cloud Computing. 18 nodes and 3 servers are included in the scenario. The simulation time per second is displayed on the horizontal axis, whereas the network average packet loss (packet loss/sec) is displayed on the vertical axis. The network average packet loss (packet loss/sec) presence of 'no firewall and no VPN' is represented by the square line while network average packet loss (packet loss/sec) presence of 'with firewall no VPN' is signified by circle line, whereas the network average packet loss (packet loss/sec) presence of 'with firewall and with VPN' is signified by triangle line. With the practice of 'firewall and no VPN', the average packet loss was greater in comparison with 'no Firewall no VPN' and 'with firewall and with VPN' because the firewall has blocked the traffic of Http and it is allowed for only users of VPN but all other clients can't access traffic of Http. So, all packets of Http are dropped. The influence of firewall and VPN on cloud computing is displayed in results. It has been verified from the graph that average packet loss is greater in case of scenario 'with firewall and no VPN' as compared to the presence of 'no firewall no VPN' and 'with firewall and VPN' in a network of cloud-based computing. It is examined by wide simulation that firewall and VPN affect network performance of cloud though it provides better security.

B. *Average Http Traffic Comparison of No Firewall No VPN, with Firewall No VPN and with Firewall VPN*

Firewall blocked the traffic of Http while at VPN side Http traffic was simply allowable for users. Those users who are not using the service of the VPN tunnel cannot able to access Http traffic from the servers as the traffic was filtered by the firewall and tested that this request was of VPN. If those users were of VPN then they were allowable by a firewall to access the traffic of Http from the servers.

1) Server AA Average http traffic received: The server AA average Http traffic received the number of requests that were made by the user to server AA that was a part of a Cloud-based computing network. The server AA Http traffic received was presented in bytes per second (bytes/sec).

TABLE. IV. RESULT OF AVERAGE PACKET LOSS FOR NO FIREWALL NO VPN, WITH FIREWALL NO VPN AND WITH FIREWALL VPN

Time	Average Packet loss (Packet per second)		
	No Firewall No VPN	Firewall No VPN	Firewall VPN
0	0	0	0
50	1.94444	1.94444	1.94444
100	1.92156	1.94117	2.00000
150	2.01923	2.73202	2.48366
200	1.95588	3.16176	2.53921
250	1.97222	3.26190	2.47222
300	1.656667	2.93333	2.09000

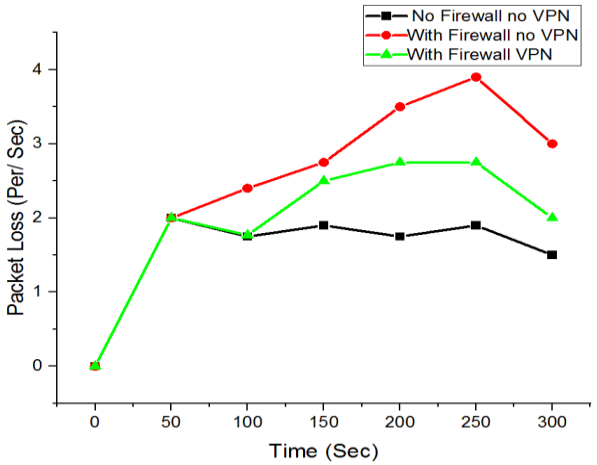

Fig. 12. Simulation Result of Average Packet Loss for No Firewall No VPN, with Firewall No VPN and with Firewall and VPN.

Table V defines the server AA average Http traffic received simulation results of no Firewall no VPN, with Firewall no VPN and with Firewall VPN

Fig. 13 illustrates the Server AA average Http traffic received simulation results of 'no Firewall no VPN', 'with Firewall no VPN' and 'with Firewall and with VPN' in a network of Cloud-based computing. 18 nodes and 3 servers are included in the scenario. Between those 18 nodes, the facility was not provided to 12 nodes to access Http traffic. Only those 6 nodes were VPN users that were connected to access point-1. These users were permitted to access Http traffic in the presence of firewalls and VPN. Simulation time per second is shown on the horizontal axis, though the Server AA average Http traffic received (bytes/sec) is displayed on the vertical axis. The Server AA average Http traffic received is displayed with the square line in the presence of 'no firewall no VPN' and the Server AA average Http traffic received is displayed with the help of circle line in the presence 'with firewall no VPN', while the Server AA average Http traffic received is shown with triangle line in the presence of firewall and VPN. In the presence of a VPN and firewall, the Server AA average Http traffic received was minimum in comparison with 'no firewall and no VPN', and the result shown in the graph is zero 'with a firewall and no VPN' as when the firewall is implemented for Http there are no facilities of VPN so no transmission took place between client and server. The results show the impact of firewall and VPN on Server AA in a network of Cloud-based computing. It has been revealed from the graph that the presence of 'no firewall and no VPN' give maximum Server AA average Http traffic received than the presence of 'with Firewall no VPN' and 'with Firewall and with VPN' in a network of cloud-based computing. Through extensive simulations It was showed that firewall and VPN affect the performance of the cloud however it gives better security.

2) Server AA Average http traffic sent: The server AA average Http traffic sent to represent the amount of data sent by the servers and received by the users which are present in the cloud computing network. The server AA average Http traffic sent is represented in bytes per second (bytes/sec).

TABLE. V. RESULT OF SERVER AA AVERAGE HTTP TRAFFIC RECEIVED FOR NO FIREWALL NO VPN, WITH FIREWALL NO VPN AND WITH FIREWALL VPN

Time	Server AA Average Http Traffic Received (bytes/sec)		
	No Firewall No VPN	Firewall No VPN	Firewall VPN
0	0	0	0
50	0	0	0
100	31.53153	0	18.91892
150	86.9281	0	64.05229
200	75.4902	0	49.03382
250	68.05556	0	40.2778
300	57.16667	0	33.83333

Fig. 13. Simulation Result of Server AA Average http Traffic Received for No Firewall No VPN, with Firewall No VPN and with Firewall VPN.

Table VI defines the server AA average Http traffic sent simulation results of no Firewall no VPN, with Firewall no VPN and with Firewall VPN in a network of Cloud.

Fig. 14 shows the server AA average Http traffic sent comparison of 'without Firewall and VPN', 'with Firewall and no VPN' and 'with Firewall and VPN' in the cloud computing network. 18 nodes and 3 servers are included in the scenario; among these 18 nodes, the 12 nodes do not have the accessibility to access Http traffic as just 6 nodes of VPN that were connected to access point-1 were the VPN users. They were only allowable to access Http traffic in the presence of a firewall with the help of VPN. The simulation time/second is showed on the horizontal axis, whereas the Server AA average Http traffic sent (bytes/sec) is shown on the vertical axis. The Server AA average Http traffic sent is displayed with the square line in the presence of 'no firewall no VPN' and the Server AA average Http traffic sent is presented with the circle line in the presence of 'firewall no VPN', whereas the Server AA average Http traffic sent is presented with triangle line in the presence of 'VPN and firewall'. The Server AA average Http traffic sent was minimum in the presence of a firewall and VPN as compared to 'no firewall and no VPN'. And the graph for 'with firewall and no VPN' is zero as whenever employing the firewall for Http 'without VPN so no Http communication was achieved between server and nodes. The results show the impact of firewall and VPN on server AA in a cloud computing network. From the graph, it has been verified that the presence of no firewall no VPN gives maximum server AA average Http traffic sent than the presence of 'with firewall no VPN and 'with firewall and VPN in a cloud computing network. Through extensive simulations, it was observed that firewall and VPN affect cloud performance while it gives better security.

TABLE. VI. RESULT OF SERVER AA AVERAGE HTTP TRAFFIC SENT FOR NO FIREWALL NO VPN, WITH FIREWALL NO VPN AND WITH FIREWALL VPN

Time	Server AA Average Http Traffic Sent (bytes/sec)		
	No Firewall No VPN	Firewall No VPN	Firewall VPN
0	0	0	0
50	0	0	0
100	18.65766	0	10.27027
150	58.88889	0	45.48366
200	51.60784	0	36.56373
250	46.3373	0	29.59921
300	38.92333	0	24.86333

Fig. 14. Simulation Result of Server AA Average http Traffic Sent for No Firewall No VPN, with Firewall No VPN and with Firewall VPN.

V. CONCLUSION

In this paper, the research work links the VPN and Firewall effect on the performance of cloud computing. The cloud computing network is simulated and evaluated for without firewall and VPN with the help of OPNET modeler 14.5; and then compared and analyzed the performance of Cloud computing after deploying "with firewall and without VPN" and "with firewall and with VPN" in term of average throughput, average end-to-end delay and average packet loss. The simulation results indicated that average throughput and average end-to-end delay of the network was decreased when implementing firewall and VPN. It seemed from the results that IP VPN is a properly effective method for transferring of data over the Cloud computing network because it provides a suitable level of security and the end-to-end delay is unaffected in the network. Besides, simulation results also revealed the fact that the average packet loss increases with the presence of VPN and firewall. From the analysis, it is concluded that deploying the firewall and VPN slightly affects the performance of Cloud computing network while it gives better security.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, vol. 1, pp. 7-18, 2010.

[2] A. Shawish and M. Salama, "Cloud computing: paradigms and technologies," in Inter-cooperative collective intelligence: Techniques and applications, ed: Springer, 2014, pp. 39-67.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," National institute of standards and technology, vol. 53, p. 50, 2009.

[4] R. Kumar, N. Gupta, S. Charu, K. Jain, and S. K. Jangir, "Open source solution for cloud computing platform using OpenStack," International Journal of Computer Science and Mobile Computing, vol. 3, pp. 89-98, 2014.

[5] A. E. Youssef, "Exploring cloud computing services and applications," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, pp. 838-847, 2012.

[6] P. Sareen, "Cloud computing: types, architecture, applications, concerns, virtualization and role of it governance in the cloud," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013.

[7] V. Chang, "Towards a Big Data system disaster recovery in a Private Cloud," Ad Hoc Networks, vol. 35, pp. 65-82, 2015.

[8] B. D. Cohen and B. L. Greenlaw, "Designing a Modern Software Engineering Training Program with Cloud Computing," 2017.

[9] S. Goyal, "Public vs private vs hybrid vs community-cloud computing: a critical review," International Journal of Computer Network and Information Security, vol. 6, p. 20, 2014.

[10] R. Buyya, S. N. Srirama, G. Casale, R. Calheiros, Y. Simmhan, B. Varghese, E. Gelenbe, B. Javadi, L. M. Vaquero, and M. A. Netto, "A manifesto for future generation cloud computing: research directions for the next decade," ACM computing surveys (CSUR), vol. 51, p. 105, 2018.

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," Communications of the ACM, vol. 53, pp. 50-58, 2010.

[12] M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future generation computer systems, vol. 28, pp. 833-851, 2012.

[13] D. Teneyuca, "Internet cloud security: The illusion of inclusion," Information Security Technical Report, vol. 16, pp. 102-107, 2011.

[14] A. Joint, E. Baker, and E. Eccles, "Hey, you, get off of that cloud?," Computer Law & Security Review, vol. 25, pp. 270-274, 2009.

[15] Adil Khan and Jiang Feng, "Mobile Sink Random Mobility Model Impact in Wireless Sensor Nodes Energy Consumption Efficiency", International Review of Basic and Applied Sciences (IRBAS), Vol. 4, Issue 12, pp. 317-325, 2016.

[16] S. Y. Ameen and S. W. Nourildean, "Firewall and VPN investigation on cloud computing performance," International Journal of Computer Science and Engineering Survey, vol. 5, p. 15, 2014.

[17] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The eucalyptus open-source cloud-computing system," in Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on, 2009, pp. 124-131.

[18] B. Harris, "Firewalls and virtual private networks," 1998.

[19] P. Gupta and A. Verma, "Concept of VPN on cloud computing for elasticity by simple load balancing technique," International Journal of Engineering and Innovative Technology, pp. 274-278, 2012.

[20] A. Malik and H. K. Verma, "Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic," International Journal of Computer Applications, vol. 46, pp. 25-30, 2012.

[21] H. Farman, B. Jan, M. Talha, A. Zar, H. Javed, M. Khan, A. U. Din, and K. Han, "Multicriteria-Based Location Privacy Preservation in Vehicular Ad Hoc Networks," Complexity, vol. 2018, 2018.

[22] H. Bourdoucen, A. Al Naamany, and A. Al Kalbani, "Impact of implementing VPN to secure wireless lan," World Academy of Science, Engineering and Technology, vol. 51, pp. 625-630, 2009.

[23] R. Buyya, S. N. Srirama, G. Casale, R. Calheiros, Y. Simmhan, B. Varghese, E. Gelenbe, B. Javadi, L. M. Vaquero, and M. A. Netto, "A manifesto for future generation cloud computing: Research directions for the next decade," ACM computing surveys (CSUR), vol. 51, pp. 1-38, 2018.

[24] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," International Journal of Information Security and Privacy (IJISP), vol. 4, pp. 36-48, 2010.

[25] A. R. Khakpour and A. X. Liu, "First step toward cloud-based firewalling," in 2012 IEEE 31st Symposium on Reliable Distributed Systems, 2012, pp. 41-50.

[26] F. Parkar and K. Wong, "Analysis of IP VPN Performance."

[27] S. Yu, R. Doss, W. Zhou, and S. Guo, "A general cloud firewall framework with dynamic resource allocation," in 2013 IEEE International Conference on Communications (ICC), 2013, pp. 1941-1945.

[28] J. Cropper, J. Ullrich, P. Frühwirt, and E. Weippl, "The role and security of firewalls in iaas cloud computing," in 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 70-79.

[29] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, pp. 1250-1258, 2017.

[30] G. Fylaktopoulos, M. Skolarikis, I. Papadopoulos, G. Goumas, A. Sotiropoulos, and I. Maglogiannis, "A distributed modular platform for the development of cloud-based applications," Future Generation Computer Systems, vol. 78, pp. 127-141, 2018.

[31] P. E. Idoga, M. Toycan, H. Nadiri, and E. Çelebi, "Assessing factors militating against the acceptance and successful implementation of a cloud-based health centre from the healthcare professionals' perspective: a survey of hospitals in Benue state, northcentral Nigeria," BMC medical informatics and decision making, vol. 19, p. 34, 2019.

AUTHORS' BIOGRAPHIES

Hussain Shah received MS degree as Gold medalist from the Institute of Computer Science & Information Technology, University of Agriculture Peshawar, KP, Pakistan. He is a PhD Scholar at the Department of Computer Sciences, Islamia College University Peshawar, KP, Pakistan. Currently, He is a Lecturer at the School of Computer Science, Shaykh Zayed Islamic Centre, University of Peshawar, KP, Pakistan. He is interested in Wireless Sensor Networks, Mobile Ad-hoc Networks, IoT, Cloud Computing and Image Processing.

Dr. Aziz-ud-Din received MS from University of Peshawar, KP, Pakistan, and PhD from UNIMAS Malaysia. He is currently working as an assistant professor at the School of Computer Science, Shaykh Zayed Islamic Centre, University of Peshawar, Peshawar, KP, Pakistan. He is interested in NLP, Mobile Ad-hoc Networks, IoT and Distributed system.

Abizar received MS degree from IBMS, Agriculture University of Peshawar. He is a PhD Scholar at the Department of Computer Sciences, Islamia College University Peshawar, KP, Pakistan. Currently, he is working as a Lecturer at the School of Computer Science, Shaykh Zayed Islamic Centre, University of Peshawar. His area of Interest includes WSN, Mobile Ad-hoc Networks, IoT and Smart Transportation. His Open researcher contribution identification (ORCID ID) is https://orcid.org/0000-0001-9472-6846.

Adil Khan received C.T. from AIOU Islamabad, B. Ed from the University of Peshawar, BS Honors in Computer Science from Edwards College Peshawar, M.S in Computer Science from City University of Science and Information Technology Peshawar and PhD from the University of Peshawar, Peshawar, KP Pakistan. He has over ten years of teaching, research and laboratory experience. In 2014-2016, he was a Senior Lecturer in Higher Education Department, Government of Khyber Pakhtunkhwa, Pakistan and in 2016-2019 he was a research scholar at the School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001 PR China. Currently, Adil khan is working as an Assistant Professor at the School of Computer Science, SZIC, University of Peshawar. He has published many publications in top-tier academic journals and conferences. He is an Associate Editor and Reviewer for several journals. Adil Khan is interested in Cloud Computing, Machine Learning, Neural networks, Game Artificial Intelligence (Game-AI), Computer Vision, Image Processing (Breast Cancer Detection) and Social Network Analysis & Mining. His Open researcher contribution identification (ORCID ID) is http://orcid.org/0000-0003-2862-5718.

Shams ud Din received MS from Islamia College University Peshawar. He is pursuing a PhD at the Department of Computer Science, Islamia College University, Peshawar, Pakistan. Currently, he is working as a Lecturer at the same Department. His fields of interest include Cloud Computing, IoT, Computer Vision, digital image processing, and Machine Learning.