Performance evaluation of multi-cloud compared to the single-cloud under varying firewall conditions

Mahbuba Yeasmin¹, Nahida Akter¹, Mohammed Humayun Kabir¹ and Javed Hossain¹

Abstract: The main purpose of this paper is to evaluate the network performances of multi-cloud compared to the single cloud under several firewall scenarios. Riverbed Modeler is used as the simulation tool in this project, and several projects are formed in this context. The projects consist of single cloud with single server, single cloud with multiple servers, multiple clouds with single server, and multiple clouds with multiple servers. In the first project, there are two scenarios: first, no firewall security across the cloud; second, the actual firewall implementation and this particular firewall allows all the required traffic. The second, third, and fourth projects were simulated with no security across the cloud, actual firewall security, and the third scenario deals with the firewall implementation that discards the web traffic. Database, web, e-mail, and file transfer applications are used as the required...
applications across the cloud to generate the traffic and the firewalls will act on these applications. The simulation results in the improvement of high performance of multiple clouds with firewall reducing the load request time, average response time, and Ethernet delay.

**Subjects:** Computing and IT Security; Distributed Network Systems; Communication Technology;

**Keywords:** cloud computing; single cloud; multi-cloud; cloud security; firewall

1. **Introduction**

Cloud networking is a term of accessing of networking resources in distributed computing systems using wide area networking or Internet-based access technologies. Cloud computing makes it easier for users and enterprises to store and process big data either in a privately maintained cloud or on a third-party server placed in a data center, which makes the data-accessing mechanisms more effective and reliable. Cloud computing counts on sharing of resources to achieve consistency and economy of scale, comparable to a utility (Armbrust et al., 2010). Providing several potential benefits and profits in organizations as well as economy, cloud computing network still has a lot of vulnerable issues that affect the model of reliability and pervasiveness. Secured cloud in heavy traffic with low latency, low response time, and no delay has become a challenging issue for the researcher as well as the network designer (Mukherjee et al., 2017). Moreover, some open issues can be diminished by choosing the type of cloud-like single or multi-computing. As an example, if we consider the issues of vendor lock-in and the matter of flexibility of using multiple application services within an organizations, then multi-cloud is the best solution, but if the main concern of cloud is to maintain the security and compliance issues of data storage or other services, then the decision of moving to multi-cloud is making the systems and IT strategies more complex and expensive. Besides the cloud sprawl is a crucial part of successfully managing a multi-cloud environment (2017). So in this paper we have studied both single- and multi-cloud network architecture and analyzed their performance based on several matrices like response time, delay, traffic received and sent, etc. We designed and simulated both networks with several server configurations providing database, e-mail, and http services under varying firewall conditions. The main aim is to create these cloud network systems and compare with each other so that an optimum cloud network system can be evaluated.

2. **Literature review**

There are many studies and works done on cloud computing architectures and its security challenges and issues. The Cloud Computing Use Case Discussion Group (2010) studied different case scenarios and discussed different risks and rewards that may exist in the cloud computing model by considering different perspectives including customers, developers, and security engineers. Popovic and Hocenski (2010) discussed the security of Service Level Agreement (SLA)'s specifications and objectives linked to data locations, isolation, and data recovery. The high-level security issues in the cloud computing model such as data integrity, payment, and privacy of sensitive information are discussed in Kandukuri, Paturi, and Rakshit (2009). The authors discussed different security management standards such as Information Technology Infrastructure Library (ITIL), ISO/IEC 27001, and Open Virtualization Format. ENISA (2009) studied the different security risks related to implementing cloud computing, along with the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. Related efforts are discussed in “Top Threats to Cloud Computing” by Cloud Security Alliance (CSA, 2010). Salman (2015) presents some multi-cloud security challenges and present adopted solutions with advantages and disadvantages. They suggested a Storage and Retrieval algorithm and cryptography-based approaches for multi-cloud, which is the easiest one to implement but the cost might be the highest for its replication features. TEBAA and El Hajji (2015) placed great prominence on shifting the companies from single-cloud to multi-cloud computing by declaring that sensitive data should
not be entrusted to a single cloud to avoid depending on just one cloud provider, and switching the
cloud computing from a single cloud to multi-clouds is mandatory to fulfill data security. They
proposed a DepSky (virtual storage system) solution that ensures the availability and confidenti-
ality of data stored in different cloud providers by using the multi-clouds architecture and the
association of “the algorithm of byzantine failures tolerance, secret sharing and erasure codes
cryptographic.” Wang (2016) proposed a novel encryption algorithm called Homomorphic Higher
Degree Residue Numbers Encryption with which users can directly operate ciphertext at the
circumstance of no plaintext and it effectively protects users’ privacy. Further, it gives a model
of protecting strategy for Digital Imaging and Communications in Medicine (DICOM) in cloud
computing and may store data in a distributed way in every cloud server with the ciphertext
form. A multi-keyword search algorithm based on polynomial function is developed in Li, Li, Wei,
Yin, and Zhao (2017) and is declared as a safety inner-product method that is very effective under
a secure cloud environment. Vee (2015) worked on a simulation-based project where single-cloud
performance was tested under several firewall conditions for database and web applications. From
the simulation results, they observed that under firewall condition with web application blocking
scenario the overall performance of the database application is enhanced and also the security
across the cloud is enhanced. There are very few works done on cloud computing security and
performance in various firewall setup conditions. So in this paper our main focus is to design four
cloud models under several firewall conditions and to evaluate the performances of cloud comput-
ing so that a better cloud computing model can be established.

3. Cloud modeling and simulation

This section discusses the design of several cloud models under different firewall scenarios. The
evaluation framework in a simulated single- and multi-cloud model has been designed in a
similar method presented in Vee (2015). The models are single cloud with single server, single
cloud with multiple servers, multiple clouds with single server, and multiple clouds with multiple
servers. The four models are simulated for three scenarios: no firewall scenario, with firewall
scenario, and firewall with block web traffic. The simulation was done after setting all the
configurations for applications, profile for database application, cloud, router, server, and LAN
for every project. For router and firewall configuration, Ethernet4_slip8_gtwy router, and to link
the cloud network, IP32 cloud and PPP_DS1 links, and for LAN the 100BaseT_LAN model were
used in every design. In IP32 cloud configuration, the packet latency is set to 0.05 s, which
indicates that the maximum packet delay across the cloud due to the database applications is
50 ms. Each and every packet is processed across the cloud with this limited delay (Vee, 2015).
After setting up all the configurations, we evaluated the performance of cloud at the global
level, node level, and link level with Riverbed Modeler. All models with different scenarios are
described in the following section.

3.1. Single cloud with single server

The project is designed only for two scenarios: no firewall and with firewall conditions. The
performance matrices were tested only for one server with database application. In firewall
configuration, we fixed the router_1 as firewall and set the attributes of application to database,
proxy server deployed to yes, and keeping the latency (seconds) value to a constant value of 0.002.
The latency for database application is set to a constant value of 0.002, and this indicates that the
packet filtering is done at the firewall and thus a delay of 20 ms is incurred over the router. Here
only the network design is shown in Figure 1.

3.2. Single cloud with multiple servers

The project was tested for no firewall, with firewall, and firewall with block web access scenario. It
was performed for two servers with database and web applications, so we had to configure the
profile for both database access (heavy) and web browsing (heavy http1.1). The cloud configura-
tion was the same as the previous project, that is, single cloud with single-server cloud scenario. In
the firewall condition, the router_1 and router_2 were set as firewall_1 and firewall_2 and the
configuration was followed as in the previous scenario. In the firewall block web access scenario,
the main aim was to block the web traffic over the network and this scenario was created by duplicating the firewall scenario. Here the proxy server application was set to http and the proxy server deployed to no and no latency was kept. The network configuration is shown in Figure 2.

3.3. Multiple clouds with single server

In this multi-cloud project, the three firewall scenarios were tested for three servers, namely server_1, server_2, and server_3, with database, web browsing, and e-mail applications, respectively, through three cloud networks. In the firewall condition, we set router_1, router_2, and router_3 as firewall_1, firewall_2, and firewall_3. We configured the firewall routers according to their application such as database, http, and e-mail, and the attribute values were the same as before. In the firewall block web access mode, we only configured the firewall router_2 the same as before to block the web traffic over the network. Figure 3 shows the multiple clouds with single server.

3.4. Multiple clouds with multiple servers

The multi-cloud network setup with multiple servers is shown in Figure 4.

In this project, the scenarios were tested for four services such as database, web browsing, e-mail, and file transfer application. server_11, server_21, and server_31 were set as database, e-mail, and file transfer, respectively, and server_12, server_22, and server_32 were set as http (web browsing) server. For the firewall condition, we set router leveling with 11, 12, 21, 22, 31, and 32 as firewall, and for firewall with block web access we configured the firewall router 12, 22, and 32. The configuration of attributes on both firewall and firewall with block web access was the same as the previous scenario.
4. Results and discussion
After designing and configuring four projects with several firewall conditions for both single- and multi-cloud networks, we set the performance metrics to observe the performance of packet delivery on different levels of database, e-mail, file, and web application across the two cloud types. The performances were compared among all scenarios and the performance metrics are http page response time,
traffic received (bytes/s), and traffic sent (bytes/s) for the web application; DB query response time, traffic received (bytes/s), and traffic sent (bytes/s) for the database application; e-mail download response time, traffic received (bytes/s), and traffic sent (bytes/s) for the e-mail application; node-level statistics like server DB query response time and load; server http page response time and load; server e-mail response time; and load is also estimated for the database, web, and e-mail application. The same metrics are chosen at all the three levels like global level, node level, and link level for every scenario. The results and perspective analysis are described for each application in the following section. Since without firewall there is no security and privacy of data in cloud, we give our discussion priority to firewall and firewall with block web access first and the no firewall scenario is described in the last section with some of its performance graphs.

4.1. Results “with firewall scenario”

4.1.1. Results for database application
The total database performance through these four projects with firewall conditions is estimated as per the performance metrics chosen, and the corresponding graphs are given next. The $X$ axis shows the simulation time, and $Y$ axis shows the response time in seconds.

In Figure 5(a), we show that multiple-cloud single-server and single-cloud single-server query response time is better than the other two due to the fact that the packet latency across the firewall router is set to a constant value of 0.002 s, and thus, the delay is incurred due to the packet filtering. When the case with single server is considered, the response time is very less when compared to the multiple-server project. As there is no packet delay across the router, the response time is very quick and the application performance is enhanced. Compared to the traffic received and sent in bytes/s in Figure 5(b) and (c), multiple-cloud multiple-server and single-cloud single-server performances are much better than the others and finally multiple clouds with multiple-server performance shows improvement according to time. In Figure 5(d), the load on the database server is almost equal across all the four scenarios. But according to time increase, the performance of multiple clouds with single server is increased. This situation indicates that due to the extra firewall policies there could be some packet delay as they are filtered, but the overall burden on the server is not affected. Even if the number of work stations is increased, the same result is observed when a firewall is placed across the cloud. From the overall analysis, it can be concluded that when a single server is used with cloud the overall performance of the database server is enhanced.

4.1.2. Results for e-mail application
In this section, the detailed performance of e-mail application will be described such as e-mail download response time, e-mail traffic received (bytes/s), and e-mail traffic sent (bytes/s). It can be easily seen in Figure 6(a) that multiple clouds with single-server model has a better performance than multiple clouds with multiple-server model. Multiple clouds with single-server performance does not affect any increasing traffic in this period.

In Figure 6(b) and (c), we can see the traffic received and sent (bytes/s) of e-mail of two models. In both cases, multiple clouds with multiple-server performance is relatively better than the others. At the end point, multiple clouds with multiple-server performance shows improvement according to time.

4.1.3. Results for http application
It is observed from Figure 7(a) that http page response time is decreased with the multiple clouds with single-server model compared to the other two models. So the multiple clouds with single server takes less time for http page responding and saves time.

It is easily seen from Figure 7(b) and (c) that the http traffic received and sent graph of multiple clouds with multiple-server model is much better than the other two models, and thus the network performance is improved. In Figure 7(d), we can see that the load request
Figure 5. (a) Database query response time (seconds), (b) traffic received (bytes/s), (c) traffic sent (bytes/s), and (d) server db_query load (requests/s) for all firewall scenarios.
Figure 6. (a) E-mail download response time, (b) e-mail traffic received, and (c) e-mail traffic sent for firewall scenario

The graph is much smaller in multiple clouds with single server and we know that the more small the load request time, the network performance will be more better.

4.2. Results for firewall with blocking web access

4.2.1. Results for database application

From Figure 8, if we compare it with Figure 5, we see the outputs are good than the firewall scenario and in this case also the performance of the multiple clouds single server is better than the other two.
4.2.2. Results for e-mail application

Figure 9 shows the e-mail download response time of two models. It is easily seen that multiple clouds with single-server model has better performance compared to the multiple clouds with single multi-server model.
Figure 8. (a) DB query response time, (b) traffic received, (c) traffic sent, and (d) server DB Query Load (requests/sec) for the firewall block web access scenario.
Figure 9. E-mail download response time for the firewall block web access scenario

Figure 10. (a) DB query response time, (b) http page response time, and (c) http traffic received (bytes/s) for the no firewall scenario
multiple-server model and the response time is the same as it was in the firewall scenario. We skipped the result of e-mail traffic received and sent graphs as they exhibit the same results as in the firewall scenario.

As in this scenario firewall was set with block web access configuration, we did not find any graph for http page response time, traffic received, traffic sent, and server http load (request/s).

4.3. Results “with no firewall scenario”
We tested all the projects with no firewall conditions and got the best performance result in both single- and multi-cloud. Without firewall cloud network data are simply a victim of uncertainty and vulnerability but sometimes there are some alternative security solutions that are combined together to speed up the network performance instead of firewall security. In these studies, we did the scenario only for resulting a comparison of cloud performances among different firewall scenarios. Here we only show the database query response time, http page response time, and http traffic received graph in Figure 10. In Figure 10(a) and (b), we can see the database query and http page response time is decreased significantly, and in Figure 10(c) the traffic received is incredibly high with an increase in the number of servers. In every case, multiple clouds with single server and multiple clouds with multiple servers perform better than the single cloud.

5. Conclusion
Many organizations are now following a multi-cloud strategy because of cloud reliability assurance and vendor lock-in solutions. Multi-cloud was, and still is, appreciated as a way to avoid data loss or interruption due to a limited component failure in the cloud. In case of cloud security, firewall and firewall with some features like web block, application block, external network interrupt block, etc., can make the networks more trustworthy and secured. In this paper, the performances of single- to multi-cloud networks with three firewall scenarios were evaluated and the target was to achieve a praiseworthy performance of multi-cloud network in firewall conditions and finally succeeded in showing that multi-clouds with single server or multi-clouds with multiple servers performs much better than single cloud in firewall and firewall with block web access scenario.

Vee, A. V. R. (2015). Usage of OPNET IT tool to simulate and test the security of cloud under varying firewall conditions, graduate project report (pp. 1–63). Texas A&M University Corpus Christi.
