Research Journal of Applied Sciences, Engineering and Technology 4(10): 1343-1350, 2012
ISSN: 2040-7467

Submitted: January 03, 2012 Accepted: February 06, 2012 Published: May 15, 2012

Development of an Efficient Secured E-Learning Tool through Smart Firewall Load Balancing Technique

R. Bala Krishnan and N.K. Sakthivel
School of Computing, SASTRA University, Thanjavur-613 401, Tamil Nadu, India

Abstract: E-Learning has definite benefits over traditional classroom training. For E-Learning, various E-Learning Tools have been proposed. However, users need to wait for long time to get response from Knowledge Database, which is called as *E-Learning Data Server*, if many users are online. And providing security to this E-Server is a challenging one. To address these issues, this work has proposed an efficient E-Learning Model through Smart Firewall Load Balancing Technique. Firewall is a device which is designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. Many personal computer Operating Systems contains software-based firewalls which is used to protect the system against threats from the public Internet. Many Routers that pass data between Networks contain firewall components and, conversely, many firewalls can perform basic routing functions. Existing Firewall Technologies such as Cisco PIX Firewalls and Checkpoint FireWall-1 provide various software tools that allowing firewalls as Clustered or Grouped and these Configured Firewalls will share their loads. The main objectives of the existing technologies are to improve the Resource Utilization along with performance and Security. This is one of the serious problems. ie the required performance can't be achieved. This research work is introduced a Adaptive Scheduler, which focuses both the Performance and Security along with Resource Utilization, and also this proposed approach reduced the firewall rules, which minimize the delay and hence this proposed work improved the Throughput, which improved the E-Server Performance in terms of Throughput, Delay and Security Strength.

Key words: Adaptive scheduler, e-learning, firewall, resource utilization

INTRODUCTION

E-Learning is to classroom learning as cell phones are to a pay phone at the bus station. E-Learning allows us to learn anywhere and usually at any time. E-learning can be CD-ROM-based, Network-based, Intranet-based or Internet-based. It can include text, video, audio, animation and virtual environments. It can be a very rich learning experience that can even surpass the level of training you might experience in a crowded classroom. It's self-paced, hands-on learning.

The quality of the electronic-based training, as in every form of training, is in its content and its delivery. E-learning can suffer from a few pitfalls, such as delayed response, which may not create a very effective learning environment. And also providing Security to this E-Learning Data Server is the major challenge due to enormous threats by passive attackers. i.e. we need an efficient mechanism to handle Knowledge Database in terms of Response Time and Security.

To address these issues, this work is planned to integrate the existing E-Learning Data Server with our proposed Smart Firewall Load Balancing Technique, which is improving the performance of E-Data Server. This work would like to address a brief history about Firewall and its designing challenges.

A firewall is a device which is designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass (MyungKeun *et al*., 2010; Liu *et al*., 2008).

Many personal computer operating systems hold software-based firewalls which are used to protect the software application against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions. This work has introduced Load Balancing Technique with five firewalls, and hence the reliability of the system also could be improved. This is one of the features of this proposed study.

LITERATURE REVIEW

In this section, this study is focused to demonstrate the existing architecture of *E-Learning Data Server* with

Corresponding Author: R. Bala Krishnan, School of Computing, SASTRA University, Thanjavur-613 401, Tamil Nadu, India

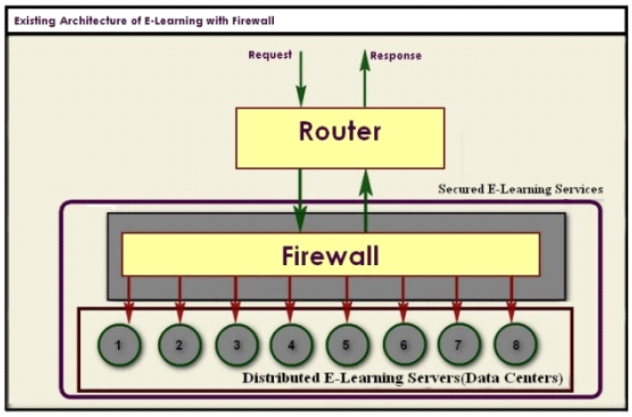

Fig. 1: Existing architecture of secured E-learning data server

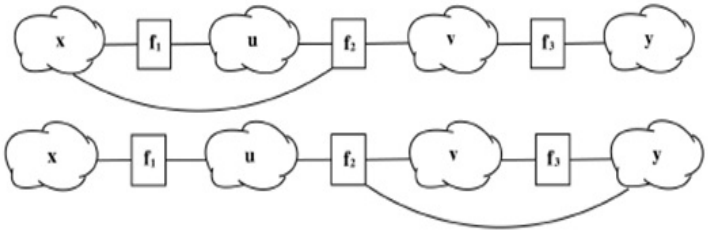

Fig. 2: Two topologies that connect domains x, u, v and y via firewalls f1, f2 and f3 set

a Firewall. The various existing Firewall Configurations, Access Control Rules and Networks Models have also been discussed in this section. The Existing E-Learning Data Server Architecture is shown in the Fig. 1. The detailed design methodology is discussed below.

Firewall configurations and its access control rules: A firewall's configuration contains a large set of access control rules, each specifying source addresses, destination addresses, source ports, destination ports, one or multiple protocol ids, and an appropriate action. The action is typically "accept" or "deny."

Some firewalls can support other types of actions such as sending a log message, applying a proxy, and passing the matched packets into a VPN tunnel (Wack *et al*., 2002); an incoming packet will be checked against the ordered list of rules. The rule that matches first decides how to process the packet. Other firewalls (such as early versions of Cisco's PIX) use the best-matching rule instead. Due to the multidimensional nature of the rules (including source/destination addresses and ports), the performance of a firewall degrades as the number of rules increases. Commercially deployed firewalls often carry tens of thousands of rules, creating performance bottlenecks in the network. More importantly, the empirical fact shows that the number of configuration errors on a firewall increases sharply in the size of the rule set.

Network models: We consider a security-sensitive enterprise network consisting of domains (subnets) that are connected with each other through firewalls. We assume that intradomain security is appropriately enforced. This work focuses on interdomain access control (MyungKeun *et al*., 2010; Wack *et al*., 2002). We further assume that dynamic routing is turned off on firewalls, while static routes are used to direct interdomain traffic, which is today's common practice in banks or other institutions that have high-level security requirements. In fact, some popular firewalls (such as many Cisco PIX models) do not support dynamic routing protocols. With static routes, robustness is achieved by using dual firewalls, which will be discussed shortly. Using static routes on firewalls is a direct consequence of the high complexity in managing the security of a mesh network. It has a number of practical advantages. First, it ensures that traffic flows are going through their designated firewalls where appropriate security policies are enforced. Second, predictable routing paths simplify the security analysis in a complex network environment, and consequently, reduce the chance of error in firewall configuration. Third, most existing dynamic routing protocols are not secure. Counterfeit routing advertisement can divert traffic through insecure paths where the packets may be copied or tampered. Note that dynamic routing is still used inside each domain as long as it does not cross an inter domain firewall. As the example in Fig. 2 shows, there are many ways to connect

x \ y	1	2	3	4	5	6	7	8
1	0	11	40	0	11	10	0	0
2	19	0	17	0	8	0	0	0
3	10	3	0	16	5	0	0	0
4	0	0	14	0	8	0	0	0
5	29	2	5	2	0	0	12	6
6	10	0	0	0	0	0	1	0
7	0	0	0	0	18	19	0	0
8	0	0	0	0	14	0	0	0

Fig. 3: Rule matrix r(x, y)

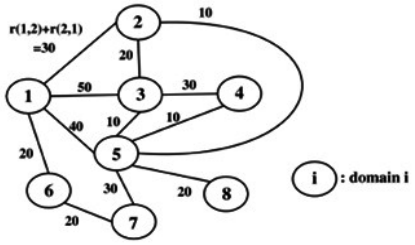

Fig. 4: Rule graph Gr

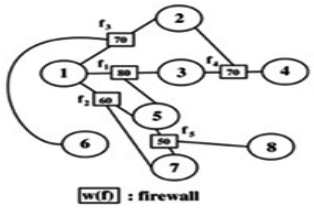

Fig. 5: Topology graph Gt

a set of domains via a set of firewalls. For any network topology, there are different ways to layout the Routing paths. In general, the rule sets to be enforced on the firewalls will be different when we change the network topology or the routing paths.

Rule graph and topology graph: This work uses the following figure to illustrate a few concepts (MyungKeun *et al*., 2010). The eight domains with IDs from 1 to 8 and the rule matrix (r(x, y), x, y $\in$ N) for the eight domains are shown in the Fig. 3.

We constructed a rule graph Gr, which is shown in Fig. 4, where each node is a domain and there is an undirected edge <x, y> if r(x, y)+r(y, x) >0.

The number of access control rules to be enforced between the two domains, i.e. r(x, y)+r(y, x), is shown beside the link. To get the output of the algorithm, we define a topology graph which is denoted as Gt. It consists of a network topology and a routing structure. A node in Gt is either a data source or domain. An undirected link (x, f) represents a physical connection between a domain x and a firewall f. This research work considers five firewalls, each having three network interfaces. The topology graph is considered for this work (MyungKeun *et al*., 2010), which is shown in Fig. 5. For this topology, the routing table is generated. A few interpretations are given below:

- Rt (1, 2) = f3 means that the routing table at domain1 has an entry for destination domain2 with the next hop being firewall f3.
- Rt (f1, 1) = 1 means that the routing table at f2 has an entry for destination domain1 with the next hop being domain1.

The complete routing interpretation for the Fig. 5 is as follows:

rt(1, 3) = f1, rt(1, 5) = f2, rt(1, 6) = f3,
rt(1, 7) = f2. rt(2, 1) = f3, rt(2, 3) = f4, rt(2, 5) = f4,
rt(3, 1) = f1,
rt(3, 4) = f4, rt(3, 2) = f4, rt(3, 5) = f1 and etc.

Identified problems: From the Previous Section, it is observed that various Mechanisms have been proposed to improve the performance of Firewalls. This section established their drawbacks and introduced efficient mechanisms to improve the performance of Firewall in terms of Load Balancing and Throughput, which will improve the performance of the E-Learning Data Server.

To improve the Firewall Performance in terms of Security and to minimize the vulnerability, researchers have introduced more policies. A large set of Policies and Access Control Rules, each specifying Source Addresses, Destination Addresses, Source Ports, Destination Ports, one or multiple Protocol IDs, and an appropriate action. The action is typically “accept” or “deny.” Due to the multidimensional nature of the rules which including source/destination addresses and ports, the performance of a firewall degrades as the number of rules increases. Firewall Technologies have been proposed to try to increase the performance by an innovative technique. Existing Technologies provide software tool that could allow firewalls to be Clustered/Grouped and therefore share the load of a busy site. From our experimental result, it is observed that this type of architecture, which is having a single Firewall, might be suitable for low volume of users. If the volume of users increases, the processing time is also increasing and hence the performance of E-Learning Data Server is degraded.

To improve the Performance along with Security, this research work is introduced an Adaptive Load Balancer, which is focusing the Utilization of Primary Firewall and the Secondary Firewalls as well (Paul *et al*., 2011; Wool, 2004). The detailed features and architecture are discussed in the next section.

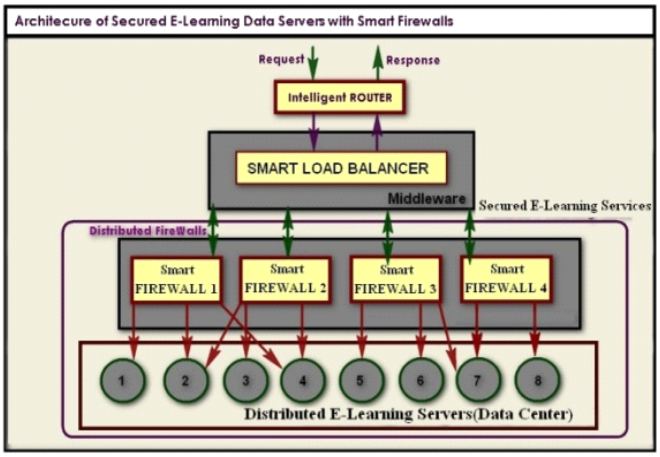

Fig. 6: Proposed architecture of secured E-learning data server

PROPOSED TECHNIQUE

The various identified problems have been listed in the previous section. To overcome these identified problems, this research work is designed an efficient Architecture, which consists of Secured E-Learning Tool with Smart Firewall, which is shown in the Fig. 6. This Architecture has two techniques namely,

- *An efficient and effective Adaptive Load Balancing Technique, which is used to optimize the load to all replicated servers*
- *Smart and Heuristic mechanism to minimize the maximum rule set*

Smart load balancer: This Adaptive Load Balancing Technique has a feature called Smart Load Balancer, which is used for two purposes.

- Used to forward request to Firewall
- Used to identify the best Firewall in Demilitarized Zone.

The procedure for the smart Adaptive Scheduler, which is the part of Load Balancer, is given below:

Accept new Call Requests

if (Utilization.FW1 < L_{Th}) then
    Forward request to FW1
If (Utilization.FW1 >= L_{Th}
and Utilization.FW2 < L_{Th}) then
    Forward request to FW2
if (Utilization.FW2 > = L_{Th}) then
    Forward request to FW3
If (Utilization.FW1 > = L_{Th}

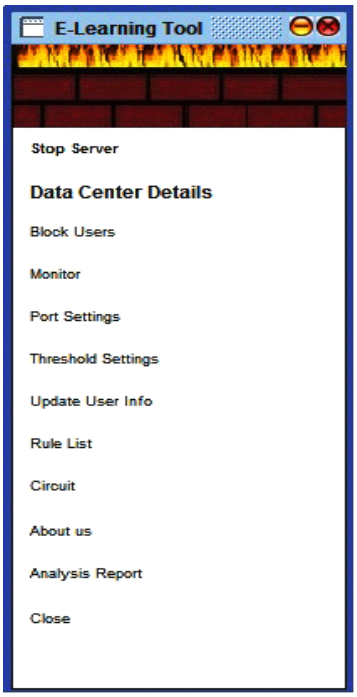

Fig. 7: Initial screen of the EL-FLUENT software. EL-FLUENT → E-Learning Tool with Firewall Load balancing rUles REductioN Technique

and Utilization.FW2 > = L_{Th}
and Utilization.FW3 < L_{Th}) then
    Forward request to FW3
if (Utilization.FW3 >= L_{Th}) then
    Forward request to FW4

Here the Threshold Limit is denoted as $L_{Th.}$ As we know, the processing time is depends upon the Primary Memory availability and number of users requests. This

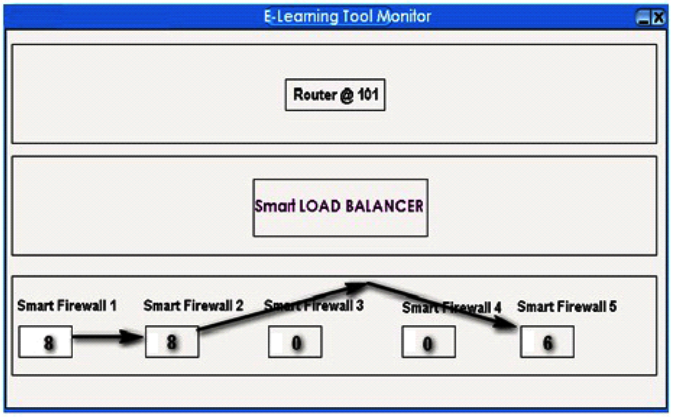

Fig. 8: Shows the E-learning tool monitoring and load transferring process

research work calculates its processing time for various levels of Primary Memory availability and number of users' requests. Based on which, the optimized threshold value is calculated. This threshold value is differing for different System configurations. This Smart E-Learning Tool along with Firewall and Smart Load Balancer is implemented with Java Programming Language and named as EL-Fluent and its Home Screen is shown in the Fig. 7.

It consists of various features such as Threshold Settings, Process Monitoring, Rules List and Port Settings etc. In Fig. 8, it is demonstrated that the procedure of Smart Adaptive Load Balancer. That is, it appears on clicking the Monitor tab of the proposed model. In this model, Router is the gateway for this application we can make the router to wait at any one of the user defined ports to receive inputs from various clients in order to access the information from the Militarized Zone. The Router will forward the incoming requests to the Smart Load Balancer, it keep tracks the status of the Smart Firewalls as per this proposed approach we have five smart firewalls.

The various Steps of Adaptive Load Balancer are listed below while forwarding the requests to Smart Firewalls.

- Read the Load value of the firewalls
- Select a suitable firewall for handling the arrived request
- Update its load value and assign the task(request) to that firewall
- Get the response from the firewall for the request
- Send the response to Router

Smart and heuristic mechanism to minimize the maximizing rule set: This mechanism has the following two schemes. They are

- Policy Optimizer (Minimize the Maximizing Rule Set of Firewall)
- Construction and Integration of Demilitarized Zone & Militarized Zone.

With the support of above stated two Schemes, the Load is sharing to all Firewalls, which is reducing the processing delay of Request and hence performance is being improved. The various rules for this proposed Smart Firewall are framed and a few rules have been shown in the Fig. 9.

The Policy Optimizer is designed in Smart and Heuristic Mechanism, which is used to perform the following activities. They are

- Early Parallel Rejection Rule (EPRR)
- Parallel Matching of Policies

It is used to view the available rules or the rules applicable in the firewall and through the rules assignment tab we can dynamically assign rules to users on the basis of the users' type.

The various policies and rules can be selected from user's option module, which is shown in the Fig. 10. We can set the applicable rules for each users as well.

Here we have the facility to block the unauthorized users on the basis of their domain names. We can set response port for each type of users so that the unauthorized persons or intruders access can be blocked.

Firewall Monitoring Technique is used to monitor the status of the Smart Firewalls. (i.e.) the system has a facility, which is used to find which smart firewall is handling the requests. Threshold settings facility is used to set both the maximum firewall limit and the threshold limit for each smart firewall. To achieve the above, this research work is designed as a Smart Firewall Framework.

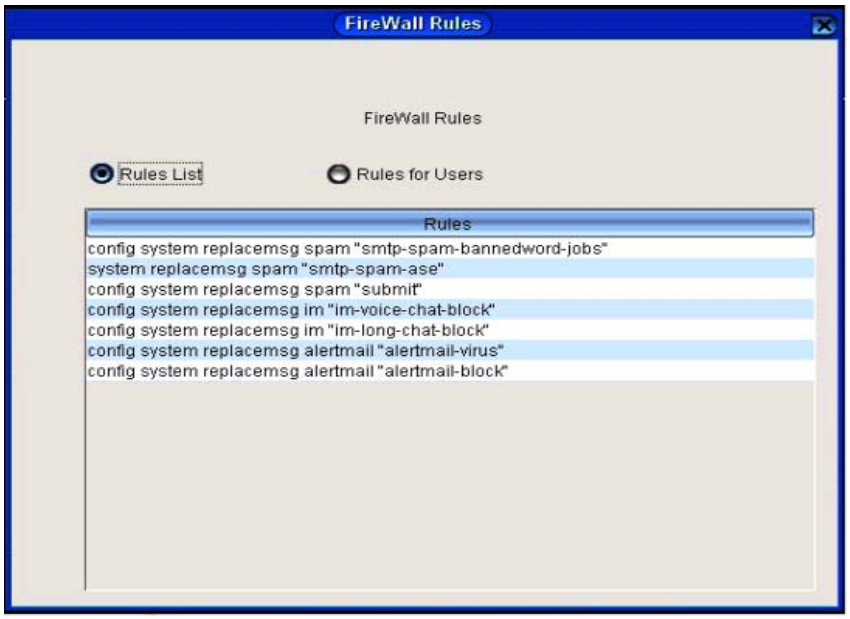

Fig. 9: Shows the rules list of the software

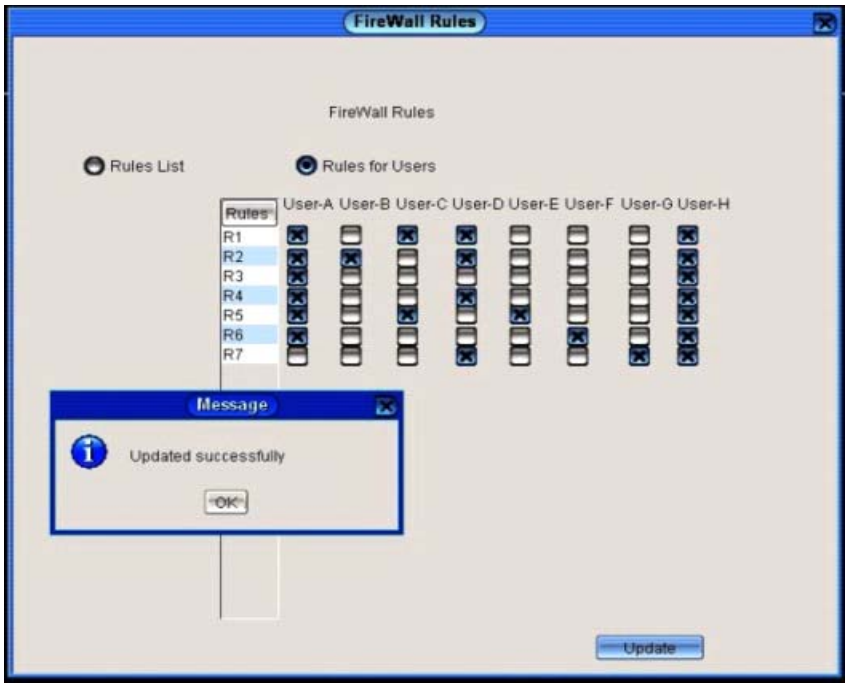

Fig. 10: Shows the rules list of the software that are assigned to various users

PERFORMANCE ANALYSIS

The EL-FLUENT firewall software is tested with various inputs from various users from various locations and the performance of the system is analyzed. In the existing firewall systems load balancing feature doesn't exist but in the proposed system we have introduced the effective load balancing feature along with firewall rules reduction policies. Rules reduction works in an effective way if more numbers of users are online.

For example, if at a particular time UserA, UserB and UserD are requesting to the firewall application in order

Table 1: Shows the list of arrived requests from various sources and the action that is either accepts

Oder	src_ip	dst_ip	dst_port	Action
1	10.0.05	20.0.0.1	20-21	accept
2	10.0.05	20.0.0.1	22-22	accept
3	10.0.05	20.0.0.1	23-25	deny
4	10.0.05	20.0.0.1	22-23	accept
5	10.0.0.0/30	20.0.0.1	80	deny
6	10.0.01	20.0.0.0/30	80	accept
7	10.0.0.0/30	20.0.0.0/30	80	deny
8	10.0.01	20.0.0.1	80-143	accept
9	10.0.0.1, 10.0.0.4	20.0.0.1	80	deny
10	10.0.0.0/24	20.0.0.0/24	any	accept
11	10.0.0.0/24	20.0.0.0/24	80	deny
12	any	any	any	deny

Table 2: Shows the concatenated requests arrivals

Oder	src_ip	dst_ip	dst_port	Action
1	50.0.0.0/26	60.0.0.0/24	80	accept
2	50.0.0.64/26	60.0.0.0/24	80	accept
3	50.0.0.128/26	60.0.0.0/24	80	accept
4	50.0.0.192/26	60.0.0.0/24	80	accept
After				
Oder	src_ip	dst_ip	dst_port	Action
1	50.0.0.0/26	60.0.0.0/24	80	accept

to access their authorized data and their usernames and password also correct but in the currently existing firewalls Rules list for UserA, UserB and UserD are checked or manipulated separately even if these users belong to same group. This proposed mechanism has Firewall-Trust mechanism, it will verify the pattern of user and if the pattern is same, for all users, the only one policy checking will be performed instead of three times, which will reduce the processing time and hence the throughput/response time will be increases, which is improving the performance of the system. This application works efficiently not only in the situation where all the rules are common for users but also it works well if some of the rules between the users are different. It check and finalizes the common rules applicable for all the users and the common rules will be checked once and all other user specific rule will be checked individually. The request will be either accepted or rejected on the basis of the rules, which is shown in the Table 1.

The Firewall Processing analyzed report is shown in the Table 2, which shows the status of the concatenated arrival of requests.

Threshold level plays a vital role in the process of handling requests by firewall.

That is for different Threshold value, the performance of the Firewall/Processor will vary, which demonstrated in the Fig. 13. The threshold value is finalized / calculated by reading the time required for each individual request and the performance percentage. This was tested on the basis of the system configuration such as RAM Size, Cache Size, Processor Speed and etc. From the Fig. 13, it is observed that the system achieves best performance if the number of request is very low and if the number of requests increases then memory utilization will also be increased and performance of the system is decreased.

From this result, it is observed that this proposed system is an effective and efficient model to improve the performance of E-Learning Data Servers, if more users approach Server. That is this model improves the performance of heavily loaded E-Learning Servers.

CONCLUSION

E-Learning is the wonderful approach and it provides more benefits over traditional classroom training. To implement E-Learning Server, various Tools have been proposed. However, from our experimental result, it is observed that users need to wait for long time to get response from E-Learning Data Server so called Knowledge Database, if many users are requesting Server. And providing security to this E-Server is also a challenging one. To address these issues, this work has proposed an efficient E-Learning Model through Smart Firewall Load Balancing Technique. From our

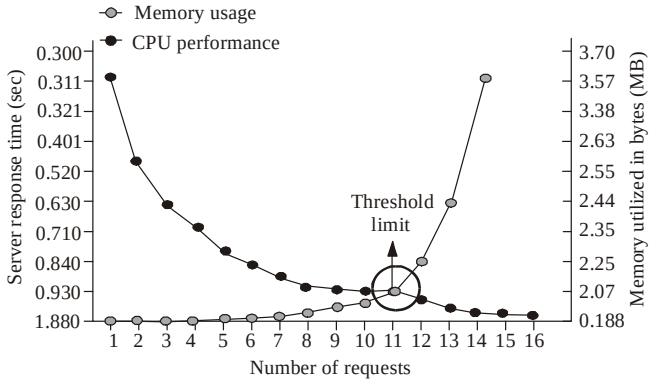

Fig. 13: Arrived requests and their corresponding memory usage and CPU performance

experimental result, it is observed that this proposed system is an effective and efficient model to improve the performance of E-Learning Data Servers, if more users approach Server. That is this model improves the performance of heavily loaded E-Learning Servers. It is very suitable model for a university to launch online E-Learning Server.

REFERENCES

Liu A.X, E. Torng, and C. Meiners, 2008. Firewall compressor: An algorithm for minimizing firewall policies. Proc. IEEE INFOCOM ’08, pp: 1-8.

MyungKeun, Y., S. Chen and Z. Zhang, 2010. Minimizing the maximum firewall rule set in a network with multiple firewalls. IEEE Transact. Comput., 59(2): 218-230.

Paul, D., M. Henzinger and I. Weber, 2011. Offline file assignments for online load balancing. Informat. Process. Lett., 111: 178-183.

Wack J., K. Cutler and J. Pole, 2002. Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology, special publication, pp: 800-841.

Wool, A., 2004. A Quantitative Study of Firewall Configuration Errors. Computer, 37(6): 62-67.