IJITE INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS IN ENGINEERING (IJITE) ISSN: 2395-2946
VOLUME-13, NUMBER-02, 2016

Result Generated by Decentralized Firewall Framework Model with Queuing For Cloud

Palak Purohit, Pramod S Nair

Department of Computer Science, Medi-Caps Institute of Technology & Management

Abstract: Cloud computing is a new adaptable approach for providing higher computational power in shared medium. Cloud computing provides the distributed model based on self evaluating techniques to improve the processing capabilities of the system with lesser managerial concerns. Cloud computing is made up of client, application, platform, servers and infrastructures. This computing model delivers computation capabilities as a calculated service from above components to end users. Though a wide variety of devices and their integration are concerned, priority of handling security will go down. As the users of cloud is increasing day by day one need to handle the data, system and confidentiality issues carefully. So a new security firewall services must be added along with existing system to provide secured access and integrity issues in a cloud environment. Implementing firewall for cloud suffers from various network oriented challenges such as load balancing, scheduling, traffic divergence, filtering, controlling the rate of arrival, instance management, attack detection. Also it is very hard to estimate the response time through a centralized cloud firewall. Thus, a new directional work had been started for practically achieving the new firewall strategies for cloud. The work also aims toward achieving the resource optimizing based provisions and rules to lower the price associated with its ownership and operations.

Keywords: Cloud computing, centralized and decentralized firewall, resource optimizing, virtualization, security, unauthorized access, malicious traffic, queue.

I. INTRODUCTION

The cloud computing is playing an important role in industry and academy with the rapid development of computer hardware and software. The cloud computing is the outcome of many factors like traditional computer technology, communication technology and business mode. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability.

The resource in the cloud system is transparent for the application and the user have no idea about the place of the resource. The users can access applications and data from remote location. Resources in cloud systems can be shared among a large number of users. The cloud system could improve capacity by adding more hardware to deal with the increased load. Cloud resources are provided as a service as per the need. The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services. The amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less.

The cloud computing must guarantee the data security so that the user need not to protect their data. So the cloud computing must ensure the security of data stored in the cloud system. Many companies provide the cloud computing platform such as Google, IBM, Microsoft, Amazon, VMware and EMC [13].

The user do not know what network are transmitting the data because the flexibility and scalability of cloud system. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. The different area has different law so the security management can meet the law risk. Cloud computing service must be improved in terms of security and protection of data.

II. LITERATURE SURVEY

System security is the important element of network, firewalls have been deployed in offending malicious and suspicious attack and unauthorized access to Internet. On the end between private network and the public Internet, a firewall monitors all incoming and outgoing packets on the basis of rules to which define security. System administrators deploy filtering rules in firewall to implement security policy. Firewall policy management is a complicated task because of the complication and dependency of filtering rules.

It is moreover aggravate by the continuous evolution of network and system environments. As an example, Al-Shaer and Hamed [1] stated that existing firewall policies have anomalies and many administrators maintained it. Moreover, Wool [2] reported that examined firewall filtering rules gathered from different organizations stating about the security flaws in firewall policies. The procedure for configuring firewall is not easy task and erroneous task. Therefore, strong methodologies and techniques for policy management are important to the eminence of firewalls. Moreover, policy anomaly detection has got a great deal of attention [1], [3], [4], [5]. While performing anomaly in traffic FIREMAN[5], only monitors all preceding rules while ignoring all other.

Cloud providers have two plans for cloud consumers for computing resources, namely reservation and on-demand plans. The provisioning plans are focused by OCRP algorithm[6] and the algorithm also considered demand and cost uncertainty associated with the resources used by consumers.

It raised another problem to application providers on how to subscribe VM resources from an IaaS provider. In this paper, considering the resource provisioning problem as a two phase resource planning problem. In the first phase, aim was on finding the optimal long term resource provisioning. For finding optimal provisioning some mathematical formulas were generated in order to calculate the optimal long term resource configuration and to reduce additional operational cost. In phase two, devise the best and effective resource configuration by a Kalman filter prediction model[6], which predict resource demand, then formulate the predicated resource configuration as integer Programming problem and transform that into Unbounded Two dimensional Knapsack problem which is solved by dynamic programming or by heuristic approach. Finally, the result of experiment shows that the queuing model with decentralization achieves a better efficiency and performance.

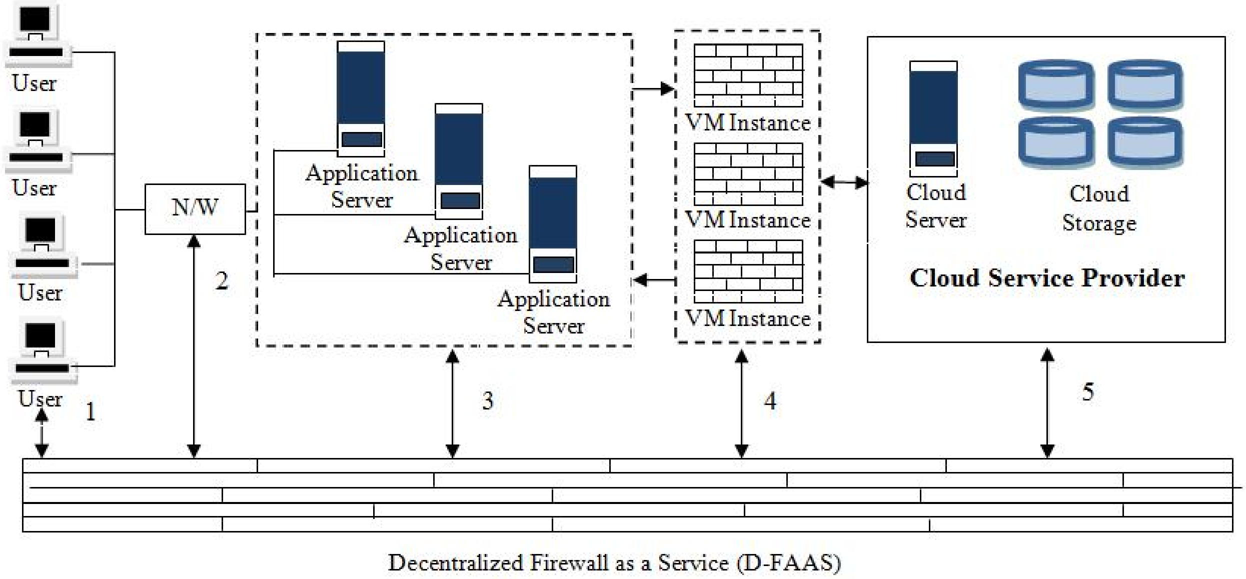
III. PROPOSED WORK

This section covers the description of new approach with in-built queuing mechanism that incorporated with firewall. Firewall maintains the queue on priority basis. The queue is divided into two classes, such that one holds the high priority request and other holds low. The high priority request is going to serve first by the cloud provider while other request will wait. We use CloudSim simulator for cloud environment.

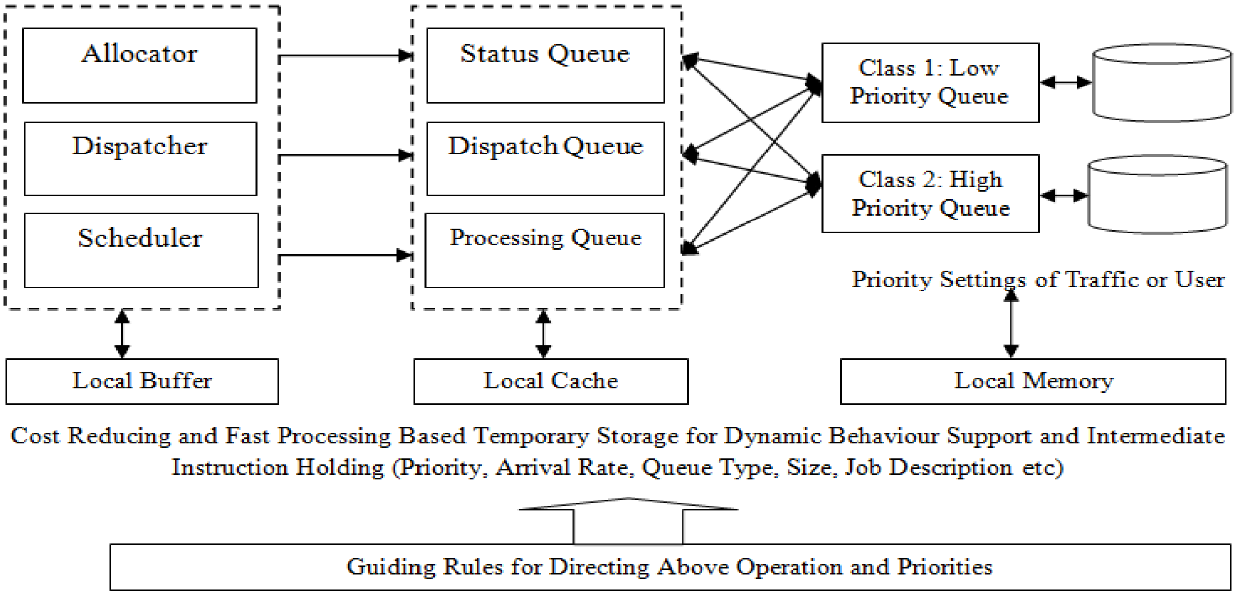
The prioritization is done on the basis of URL decomposition. The URL part of websites is consisting of following components:

URL-→ (Protocol Identifier, Resource name, Domain name)

In proposed work, we worked on Protocol identifier. The architecture is shown below:



(A) Decentralized Firewall as a Service (D-FAAS) Applicability Model (1 to 5)


Allocator
Dispatcher
Scheduler
Status Queue
Dispatch Queue
Processing Queue
Class 1: Low Priority Queue
Class 2: High Priority Queue
Priority Settings of Traffic or User
Local Buffer
Local Cache
Local Memory
Cost Reducing and Fast Processing Based Temporary Storage for Dynamic Behaviour Support and Intermediate Instruction Holding (Priority, Arrival Rate, Queue Type, Size, Job Description etc)
Guiding Rules for Directing Above Operation and Priorities

(B) D-FAAS Architecture with Improved Queuing System Using Dynamic Support

Decentralized firewall deployment requires dynamic resource allocation and de-allocation with continuous monitoring. With a switching of multiple VM instances it is practically infeasible by CSP to satisfy these requirements. Also, the traditional mechanism is maintaining the regular queue of jobs to be processed through the model M/G/1 which uses Markov chain. It uses two classes for organizing their priority scheduling. In proposed approach the class 1 holds the low priority based data and the class 2 holds the high priority based data. Here the queue only allows one class 2 customers at a time and this class is having no buffer arrangements for holding more high priority instructions.

IV. RESULT ANALYSIS

The aim is towards providing more security and robustness against the traditional issues of centralized firewall. It proves the major areas of attack and malicious behavior detection using pattern analysis or controlling access using filtration process.

Effective implementation of distributed firewall can be achieved by accessibility and dependency analysis of the user's traffic. If the system provides effective access control but let's open the trapdoors for the malicious user then the confidentiality of the system can be loosed. It has a risk associated with the cloud based outsourced environment. Also the control must be regularly monitored and verified against each minute detail such as response time etc. The proposed firewall can achieve following benefits over the traditional centralized firewall.

- **Time Consumption**

  The amount of time required to process the request using the selected algorithm is known as time consumption of the system.

The figure 1 shows the comparative time consumption of traditional and proposed approach. According to the graph X axis shows the number of request on cloud with and the Y axis shows the amount of time consumed in serving the request in seconds. Thus in the parameter of time consumption or time complexity the performance of proposed model is better as compared to the centralized.

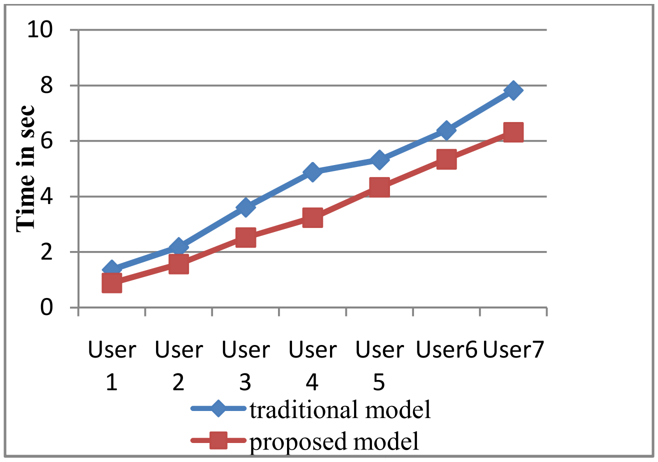


Figure 1: Time Consumption

- **CPU Consumption**

Figure 2 below shows the consumption of CPU of system with our model and without our model.

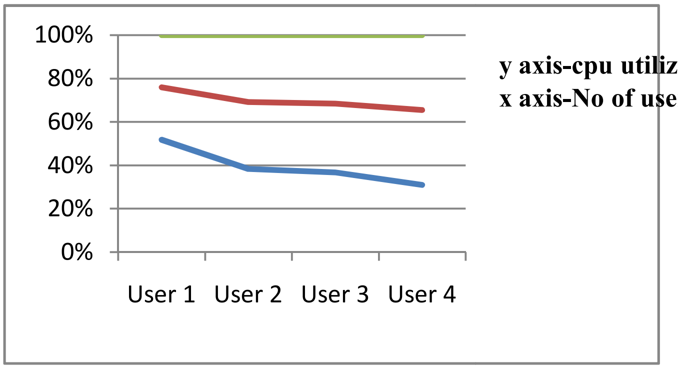


Figure 2: CPU Consumption

IV.CONCLUSION

Cloud computing is growing technology which gives higher computational power in shared medium. It provides distributed model based on self assessing systems to increase the processing abilities of the system with lesser managerial concerns. It consist of client, application, platform, servers and infrastructures. Security has to add alongside existing system to provide secured access and uprightness issues in a cloud environment. Actualizing firewall for cloud experiences different network oriented challenges, for example, load balancing, scheduling, traffic divergence, filtering, controlling the rate of entry, instance management, attack detection. The given model performance is good in time and load balancing as having priority queue in it

The table shows the overall result of proposed model and traditional model.

Table 4.1

	Attribute Name	**Data Sources**	**Operations**	**Centralized Firewall**	**Distributed Firewall (Priority Queue)**
1	Attack Routes	Network Traffic	Response Time Delay	High	Low
2	Host Behaviour	Scan Information	Criticality Level and Priority Settings	No	Yes
3	Attack Impact	IDS Alerts	Low Complexity Capturing & Lightweight Execution	No	Yes
4	Threat Level	IDS Alerts	Traffic Classification with Packet Tagging	No	Yes
5	Network Configuration	Network Traffic	Network Bandwidth Consumption	High	Less

V. FUTURE WORK

In future we can work on the varieties of the rules including more number of static and dynamic aspects that can be used to fulfill the requirements of the user. We can work on rest two component of URL. It means we can set more filtering rules on IP address and domain name to avoid conflicts if any.

REFERENCES

[1] H Hu, Student Member, IEEE, G J Ahn, Senior Member, IEEE,"Detecting and Resolving Firewall Policy Anomalies" IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 3, May/June 2012

[2] D Chen1,H Zhao1, "Data Security and Privacy Protection Issues in Cloud Computing" published in 2012 International Conference on Computer Science and Electronics Engineering IEEE DOI 10.1109/ICCSEE.2012.193.

[3] M Liu, Student Member, IEEE, W Dou, Member, IEEE, S Yu, Senior Member, IEEE, and Z Zhang, Senior Member, IEEE "A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization" publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TPDS.2014.2314672, IEEE

Transactions on Parallel and Distributed Systems in 2014

[4] S Chaisiri, Student Member, IEEE, B S Lee, Member, IEEE, and D Niyato, Member, IEEE, "Optimization of Resource Provisioning Cost in Cloud Computing" published in IEEE Transactions On Services Computing, Vol. 5, No. 2, April-June 2012.

[5] Balaji Palanisamy, Member, "Cost-Effective Resource Provisioning for Map reduce in aCloud" published in IEEE Transactions on Parallel and Distributed Systems 2013 IEEE.

[6] Security Guidance for Critical Areas Of Focus in Cloud Computing Vol 3.0 by Cloud Security Alliance.

[7] R H Hwang1, C N Lee2, Y R Chen1, D J Z Jian2, "Cost Optimization of Elasticity Cloud Resource Subscription Policy" IEEE Transactions on Journal Name 1939-1374/2013 IEEE

[8] K Chen, J Powers, S Guo, and F Tian, "CRESP: Towards Optimal Resource Provisioning for Map Reduce Computing in Public Clouds" published in IEEE Transactions On Parallel and Distributed Systems, Vol. 25, No. 6, June 2014

[9] Ms. Z Padiya, MS. S Kulshreshtha, Mr. K Bhimani, “Live Video Streaming On Mobile Application”, Journal of Information, Knowledge and Research in Computer Science And Applications, vol. 02, no. 02, Page 99, ISSN: 0975 – 6728, Nov 12to Oct 13.

[10] E G. Amoroso, AT&T,"Practical Methods for Securing the Cloud" IEEE Cloud Computing published by the IEEE Computer Society 2014 IEEE

[11] P Purohit, A Joshi, R Jain "Decentralized Firewall as a Service (D-Faas) Applicability Model with Improved Queuing Using Dynamic Support for Cloud" published in IJSCIT 2015.