ISSN:0975-9646

Decentralized Firewall as a Service (D-FAAS) Applicability Model with Improved Queuing Using Dynamic Support for Cloud

Palak Purohit, Awani Joshi, Richa Jain

Department of Computer Science and Engineering,
Medi-Caps Institute of Technology and Management Indore,
M.P, India

Abstract: **Cloud computing is a new flexible approach for providing higher computational power in shared medium. It provides the distributed model based on self-evaluating techniques to improve the processing capabilities of the system with lesser managerial concerns. It 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. It 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 becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode in the industry. Entirely 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 do not know the place of the resource. The users can access your applications and data from anywhere. Resources in cloud systems can be shared among a large number of users. The cloud system could improve its capacity through adding more hardware to deal with the increased load effectively when the work load is growing. Cloud resources are provided as a service on an as needed basis. The cloud itself typically includes large numbers of commodity-grade server infrastructures, committed 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 resource can be the computing, storage and other specification service. The cloud computing is seen as the important change of information industry and will make more impact on the development of information technology for the society. The majority of cloud computing infrastructure currently consists of reliable services delivered through data centre that are built on servers with different levels of virtualization technologies and approaches. Services are accessible anywhere in on the globe, The Cloud appearing as a single point of access for all thee computing needs of consumers. The cloud computing changed the style of software.

The data can be stored in the cloud system and the user can use the data in any time and in anywhere. The data often stored in the private or personal system such as PC. The cloud computing can guarantee the data security and the user do not protect the data by himself again. 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].

As the cloud computing system has more data which may be the private data of user, the data must not be destroyed or grabbed. Because the data in the cloud system may be important for the user, the hacker may pay more attention to get the data. The system must be protected more carefully than the traditional system. The company uses the cloud system and stores the data in it. The data can be seen by other people who are not person of company. The company must have confidence in the cloud computing if they want to store the private data in the cloud system. Governance and security are crucial to computing on the cloud service provider's infrastructure, if the cloud system is in firewall or not.

Understanding Cloud Security

The security of cloud computing is the key import problem in the development of cloud computing. The traditional security mechanism cannot protect the cloud system entirely. The cloud computing application is no boundaries and mobility and can lead many new security problems.

The main security issues include data security, client data security assurance, cloud computing platform dependability and cloud computing organization. The cloud system is running in the web and the security issues in the web additionally can be found in the cloud system. The cloud system is not distinctive the customary system in the PC and it can meet other uncommon and new security issues. the greatest worries about cloud computing are security and protection [9].

The customary security issues, for example, security vulnerabilities, infection and hack attack can likewise make dangers to the cloud system and can lead more genuine results in light of property of cloud computing. Programmers and pernicious intruder may hack into cloud records and take touchy data put away in cloud systems. The data and business application are put away in the cloud focus and the cloud system must ensure the resource painstakingly.

Cloud computing is an innovation advancement of the widespread selection of virtualization, administration oriented structural planning and utility computing. over the Internet and it includes the applications, platform and administrations. In the event that the systems meet the disappointment, quick recuperation of the resource additionally is an issue. The cloud systems hide the details of administration execution innovation and the management. The client can't control the advancement of deal with the data and the client can't verify the data security without anyone else. The data resource stockpiling and operation and network change likewise deals with the cloud system. The key data resource and protection data are extremely import for the client.

Data-in-flight assurance in Cloud computing

The cloud must provide data control system for the client. The data security review likewise can be deployed in the cloud system. Data moving to any approved spot you require it, in a structure that any approved application can utilize it, by any approved client, on any approved device. Data respectability obliges that just approved clients can change the data and Confidentiality implies that just approved clients can read data.

Cloud computing ought to provide solid client access control to fortify the permitting, certificate, isolate and different parts of data management. In the cloud computing, the cloud provider system has numerous clients in a dynamic response to changing administration needs. The clients don't comprehend what position the data and don't know which servers are processing the data.

The client don't comprehend what network are transmitting the data on the grounds that the adaptability and scalability of cloud system. The client can't verify data protection worked by the cloud in a confidential manner. The cloud system can deploy the cloud focus in diverse range and the data can be put away in distinctive cloud node. The distinctive territory has diverse law so the security management can meet the law hazard. Cloud computing administration must be enhanced in legitimate assurance.

II. BACKGROUND

One of essential elements in network and data system security, firewalls have been widely deployed in defending suspicious traffic and unauthorized access to Internet-based enterprises. Sitting on the border between a private network and the public Internet, a firewall examines all incoming and outgoing packets based on security rules. To execute a security policy in a firewall, system administrators define a set of filtering rules that are derived from the hierarchical network security requirements. Firewall policy management is a challenging task because of the complexity and interdependency of policy rules.

This is further exacerbated by the continuous development of network and system environments. For instance, Al-Shaer and Hamed [1] reported that their firewall policies contain anomalies despite the fact that several administrators including nine experts kept up those policies. Likewise, Wool [2] recently inspected firewall policies collected from distinctive organizations and indicated that all analyzed firewall policies have security flaws.

Firewall Configurations

The process of configuring a firewall is tedious and blunder inclined. Thusly, effective mechanisms and tools for policy management are crucial to the success of firewalls. Recently, policy peculiarity detection has received a lot of consideration [1], [3], [4], [5]. Corresponding policy analysis tools, such as Firewall Policy Advisor [1] and FIREMAN [5], with the objective of detecting policy anomalies have been introduced. Firewall Policy Advisor just has the capability of detecting pairwise anomalies in firewall rules. Fire fighter can detect anomalies among various rules by dissecting the relationships between one guideline and the collections of packet spaces derived from all preceding rules. On the other hand, FIREMAN also has limitations in detecting anomalies [3].

For each firewall tenet, FIREMAN just examines all preceding rules yet ignores all subsequent rules when performing abnormality analysis. Likewise, each analysis result from FIREMAN can just show that there is a misconfiguration between one tenet and its preceding rules, yet cannot accurately indicate all rules included in an inconsistency.

Then again, because of the complex way of policy anomalies, system administrators are frequently faced with an additionally challenging problem in determining anomalies, in particular, determining policy conflicts. An instinctive means for a system executive to determine policy conflicts is to evacuate all conflicts by altering the conflicting rules. Then again, changing the conflicting rules is significantly difficult, even impossible, in practice from numerous aspects.

First, the quantity of conflicts in a firewall is potentially substantial, since a firewall policy may consist of a huge number of rules, which are frequently logically entangled with each other. Second, policy conflicts are frequently exceptionally complicated. One guideline may conflict with multiple different rules, and one conflict may be associated with several rules. Besides, firewall policies deployed on a network are frequently kept up by more than one manager, and an enterprise firewall may contain legacy rules that are designed by diverse administrators. Subsequently, without from the earlier information on the administrators' propositions, changing rules will affect the rules' semantics and may not resolve conflicts correctly.

Moreover, now and again, a system chairman might intentionally introduce certain overlaps in firewall rules realizing that just the first govern is important. In reality, this is a commonly utilized technique to exclude specific parts from a certain action, and the proper utilization of this technique could bring about a less number of compact rules [5]. In this case, conflicts are not an error, yet intended, which would not be necessary to be changed.

Since the policy conflicts in firewalls always exist and are difficult to be eliminated, a practical resolution system is to identify which administer included in a conflict circumstance ought to come first when multiple conflicting rules (with diverse actions) can channel a particular network packet simultaneously. To determine policy conflicts, a firewall typically implements a first-match resolution mechanism based on the order of rules. Along these lines, each packet processed by the firewall is mapped to the decision of the first decide that the packet matches. In any case, applying the first-match strategy to cope with policy conflicts has restrictions.

Firewall demerits

At the point when a conflict occurs in a firewall, the existing first matching rule may not be a desired rule that ought to bring precedence with respect to conflict resolution. In particular, the existing first matching rule may perform opposite action to the rule which ought to be considered to come first. This circumstance can cause serious network breaches such as permitting harmful packets to sneak into a private network, or dropping legal traffic which thus could encumber the availability and utility of network services.

Clearly, it is necessary to look for an approach to bridge a gap between conflict detection and conflict resolution with the first-match mechanism in firewalls. In this paper, we represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate more accurate anomaly detection as well as effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments.

Each segment associated with an one of a kind set of firewall rules accurately indicates an overlap connection (either conflicting or repetitive) among those rules. We also introduce a flexible conflict resolution strategy to empower a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the danger assessment of protected networks and the intention of policy definition. Besides, a more effective redundancy end mechanism is provided in our framework, and our experimental results demonstrate that our redundancy discovery mechanism can achieve approximately 70 percent improvement compared to traditional redundancy detection approaches [1], [6].

In addition, the outputs of prior policy analysis tools [1], [5] are predominantly a rundown of possible anomalies, which does not give system administrators a clear perspective of the start of policy anomalies. Since information visualization technique [7] empowers clients to explore, analyze, reason, and explain abstract information by taking playing point of their visual cognition, our policy analysis tool adopts an information visualization technique to facilitate policy analysis. A gridbased visualization approach is introduced to represent policy anomaly analysis information in an intuitive way, enabling an efficient anomaly management.

Likewise, we implement a visualization-based firewall anomaly management environment (FAME) based on our approach. To evaluate the practicality of our tool, our extensive experiments deal with a set of real-life firewall policies.

III. Related Literature

Although cloud computing has numerous advantages, there are still numerous actual problems that need to be solved. According to a Gartner survey about cloud computing revenues, market size for Public and Hybrid cloud is $59 billion and it will reach USD 149B by 2014 with a compound annual growth rate of 20[11]. The revenue estimation implies that cloud computing is a promising industry.

At the same time from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved at the earliest opportunity. Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information.

The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The capacity to control what information to reveal and who can access that information over the Internet has become a growing concern. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements.[4]

Cloud providers can offer cloud consumers two provisioning plans for computing resources, namely reservation and on-demand plans. In general, cost of utilizing computing resources provisioned by reservation plan is cheaper than that provisioned by on-demand plan, since cloud consumer needs to pay to provider in advance. With the reservation plan, the consumer can reduce the total resource provisioning cost. However, the best advance reservation of resources is difficult to be achieved due to uncertainty of consumer's future demand and providers' resource prices.

To address this problem, an optimal cloud resource provisioning (OCRP) algorithm is proposed by formulating a stochastic programming model. The OCRP algorithm can provision computing resources for being used in multiple provisioning stages and also a long-term plan, e.g., four stages in a quarter plan and twelve stages in a yearly plan.

The demand and price uncertainty is considered in OCRP. In this paper, different approaches to obtain the solution of the OCRP algorithm are considered including deterministic equivalent formulation, sample-average approximation, and Benders decomposition. Numerical studies are extensively performed in which the results clearly demonstrate that with the OCRP algorithm, cloud consumer can successfully minimize total cost of resource provisioning in cloud computing environments.[5] Recently, IaaS infrastructure becomes a popular platform for application providers to deploy their applications. However, IaaS providers offer many types of VM configuration and price them differently. Furthermore, they also offer several pricing models.

It raises an interesting issue to application providers on the best way to effectively provision or subscribe VM resources from an IaaS provider. In this paper, we formulated the resource provisioning problem as a two phase resource planning problem. In the first phase, we focused on determining the optimal long term resource provisioning. We proposed some mathematical formulae to compute the optimal long term resource configuration to minimize the expected operational cost. In the second phase, we proposed a Kalman filter prediction model for predicting resource demand. We then formulated the optimal resource configuration for the predicted demand as an Integer Programming pro blem and transformed it to an Unbounded Twodimensional Knapsack Problem which can be solved through dynamic programming or heuristic algorithms.

Several issues had also been considered in our work, including impact of latency of VM re-configuration, and minimum rental time constraint for launching a VM. We evaluated our proposed solutions based on workload data from a real system and Amazon EC2 pricing model. Our numerical results showed that the proposed long term resource planning algorithm had the capacity yield near optimal operational cost. The results also showed that the proposed on-demand planning algorithm significantly reduced the operational cost and had the capacity cope with the latency of VM reconfiguration.

This paper presents a new MapReduce cloud service model, Cura, for data analytics in the cloud. We argued that existing cloud services for MapReduce are inadequate and inefficient for production workloads. In contrast to existing services, Cura automatically creates the best cluster configuration for the jobs using MapReduce profiling and leverages deadlineawareness which, by delaying execution of certain jobs, allows the cloud provider to optimize its global resource allocation efficiently and reduce its costs.

Cura also uses a unique secure instant VM allocation technique that ensures quick response time guarantees for short interactive jobs, a significant proportion of modern MapReduce workloads. Cura resource management techniques include cost-aware resource provisioning, VMaware scheduling and online virtual machine reconfiguration.[8]

Running MapReduce programs in the public cloud raises an important problem: how to optimize resource provisioning to minimize the monetary or time cost for a specific occupation? To answer this question, we believe a fundamental problem is to understand the relationship between the amount of resources and the employment characteristics (e.g., input data and processing algorithm).[9] Enterprise organizations and cloud service providers today are using several practical methods to secure their cloud infrastructure and services:

- A private cloud with enterprise perimeters is the most common large enterprise approach to securing cloud content.
- A public cloud with service gateways involves popular cloud services used by millions of individuals and businesses today.
- Content encryption focuses on protecting data stored in the cloud from unauthorized compromise and leakage.
- Session containers ensure that data are properly removed from client devices such as mobile devices after cloud access.
- Cloud access brokers integrate security measures such as authentication or access monitoring for users accessing cloud services.
- Runtime security virtualization integrates dynamic runtime virtual security functions directly into virtual entities in the cloud.[10] Any resource allocation model needs to consider computational resources and additionally network resources to accurately reflect practical demands.

Another aspect that ought to be considered while provisioning resources is energy consumption. This aspect is getting more attention from industrial and government parties. Calls for the support of green clouds are gaining momentum. On account of that, resource allocation algorithms mean to accomplish the assignment of scheduling virtual machines on the servers residing in data centers and consequently scheduling network resources while complying with the problem constraints.

Several external and internal factors that affect the performance of resource allocation models are introduced in this article. These factors are discussed in detail, and research gaps are pointed out. Design challenges are discussed with the point of providing a reference to be used when designing a comprehensive energy-aware resource allocation model for cloud computing data

IV. PROBLEM IDENTIFICATION

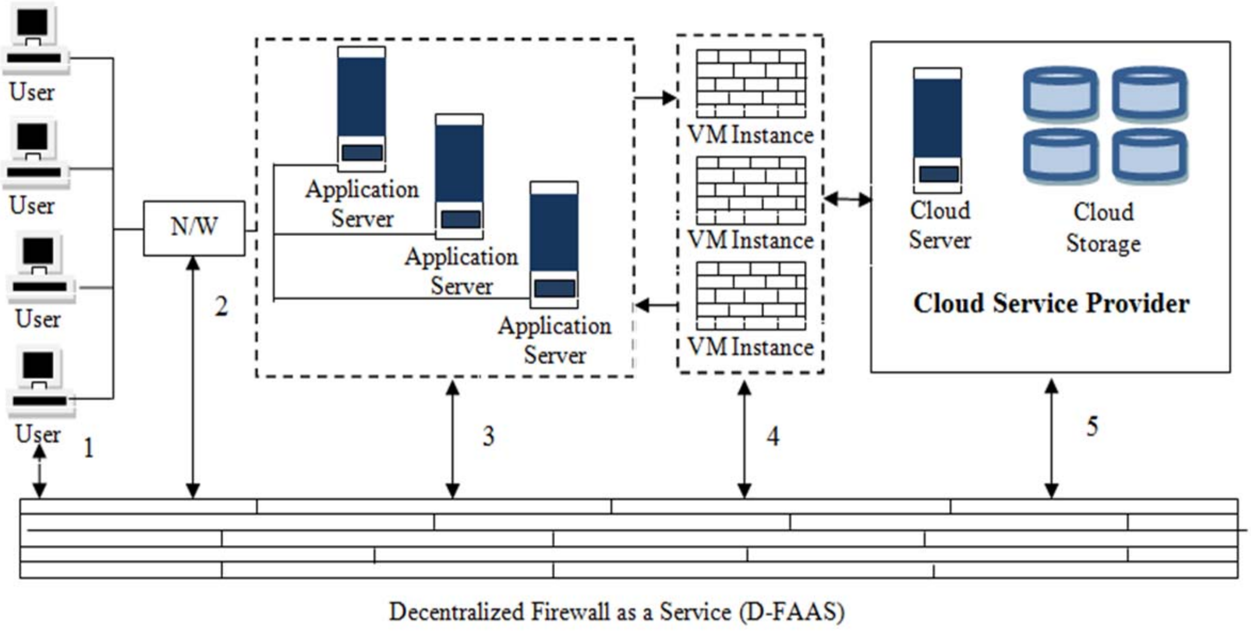
Cloud is a trusted third party service based computing having effective resource allocation policies. These policies are responsible for serving the user's needs in a controlled manner. As far as security is concerned, cloud uses some of traditional security mechanism to achieve confidentiality, privacy and attack detection.

Here the attack detection is one of the most prominent areas of work. Firewall is the most known way of detecting the unauthorized access to the system and blocks the malicious traffic. 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. After studying the various research articles, there is some mechanism which resolves these issues. But to make a centralized firewall, implementation issues makes it practically difficult task. In case of centralized firewall hosting, the VM capacity exceeds the practical achievability of resources. Single VM instance does not satisfies the QoS based customers requirements. Also it is very hard to estimate the response time through a centralized cloud firewall.

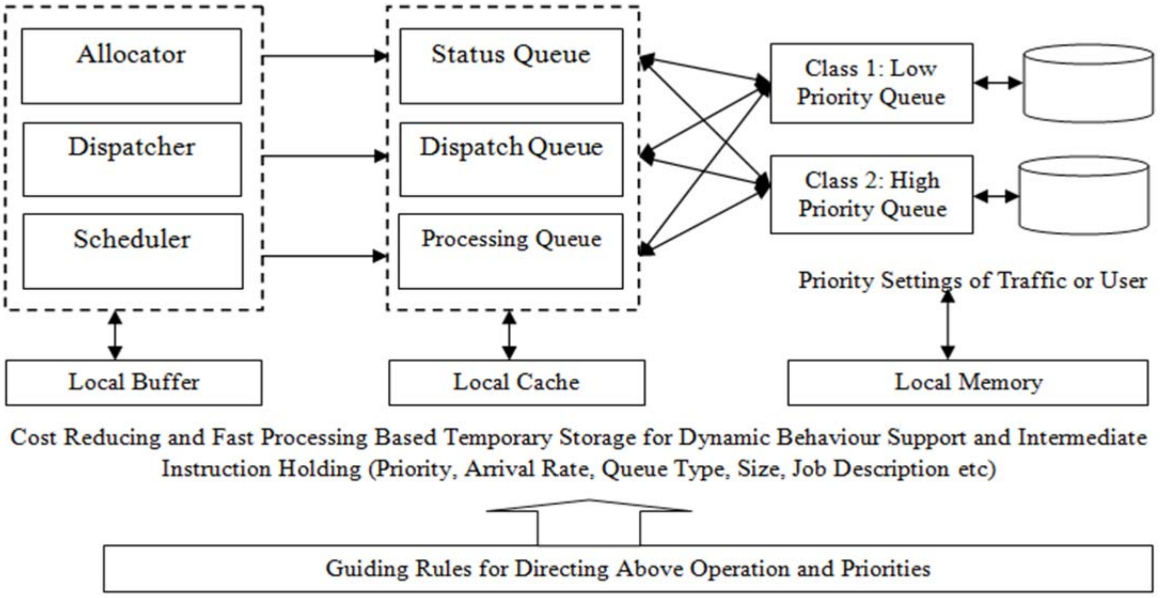
Thus, a new directional work had been started for practically achieving the new firewall strategies for cloud. Out of those the decentralized approach is serving all the key requirements. In this the multiple VM instances are operating simultaneously to provide the decentralized attack and traffic management solutions. It also aims toward achieving the resource optimizing based provisions and rules to lower the price associated with its ownership and operations. Some of its design factors are packet arrival rate, attack duration detection and reduction etc. After studying some of the research articles of working concept, the work had identified the direction are of further work with decentralized firewall for cloud. These are:

Direction of Work: 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.

Here 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. Thus it violates the scalability phenomenon's of cloud computing. While the class 1 queues is having dynamic length. Thus, the director of work identified here is to maintain the dynamic queue size for both class 1 and class 2 based on their priorities of execution.



(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

FIGURE 1: PROPOSED D-FAAS SYSTEM (A) AND (B) WITH IMPROVED QUEUING USING DYNAMIC SUPPORT FOR CLOUD

V. PROPOSED D-FAAS SYSTEM

Decentralized firewall deployment obliges dynamic resource allocation and de-allocation with constant observing. With an exchanging of numerous VM instances it is basically infeasible by CSP to fulfill these necessities. Additionally, the conventional instrument is keeping up the normal queue of occupations to be handled through the model M/G/1 which utilizes Markov chain. It utilizes two classes for sorting out their priority scheduling. Here the class 1 holds the low priority based data and the class 2 holds the high priority based data as shown in figure 1.

Here the queue just allows one class 2 customers at once and this class is having no cushion plans for holding all the more high priority directions. In this way it damages the scalability wonder's of cloud computing. While the class 1 queues is having dynamic length. In this way, the chief of work identified here is to keep up the dynamic queue size for both class 1 and class 2 based on their priorities of executions.

Here the attack detection is a standout amongst the most noticeable zones of work. Firewall is the most known method for discovering the unauthorized access to the framework and obstructs the vindictive traffic. Actualizing firewall for cloud experiences different system arranged difficulties, for example, load balancing, scheduling, traffic difference, filtering, controlling the rate of landing, instance management, attack detection. In the wake of considering the different examination articles, there is some instrument which determines these issues.

However to make a centralized firewall, usage issues makes it essentially troublesome undertaking. In the event of centralized firewall facilitating, the VM limit surpasses the commonsense achievability of resources. Single VM instance does not fulfills the QOS based customers prerequisites. Likewise it is difficult to gauge the reaction time through a centralized cloud firewall.

Hence, another directional work had been begun for essentially attaining the new firewall procedures for cloud. Out of those the decentralized methodology is serving all the key necessities. In this the different VM instances are working all the while to give the decentralized attack and traffic management arrangements.

It likewise points to attaining the resource optimizing based provisions and tenets to bring down the cost connected with its possession and operations. Some of its outline variables are bundle entry rate, attack length of time detection and diminishment and so on. In the wake of concentrating on a portion of the exploration articles of working idea, the work had recognized the course are of further work with decentralized firewall for cloud.

VI. CONCLUSION

CLOUD COMPuting is another adaptable methodology for giving higher computational power in shared medium. It provides the distributed model based on self assessing systems to enhance the processing abilities of the system with lesser managerial concerns. It is made up of client, application, platform, servers and infrastructures. This computing model delivers reckoning capacities as an issue administration from above segments to end clients. In spite of the fact that a wide mixed bag of devices and their incorporation are concerned, priority of taking care of security will go down. As the clients of cloud is expanding step by step one need to handle the data, system and confidentiality issues deliberately.

So another security firewall administrations said in the work ought to added 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. Likewise it is tricky to gauge the response time through a centralized cloud firewall. Therefore, another directional work had been begun for essentially attaining the new firewall strategies for cloud. It additionally points to attaining the resource optimizing based provisions and tenets to lower the cost connected with its ownership and operations.

ACKNOWLEDGMENT

I am especially grateful to my guide Mrs. Richa Jain, Assistant Professor, Department of Computer Science and Engineering, Medi-caps Institute of Technology and Management, Indore for her comment and direction in my research work. My sincere thanks are due to Dr. S. K. Somani, Director, Medicaps Institute of Technology and Management, Indore for individual encouraging thoughts. I express my heartfelt gratefulness to Dr. Promod Nair, HOD, Computer science and Engineering Department, Medicaps Institute of Technology and Management, Indore, for his stimulating supervision.

REFERENCES

[1] Meng Liu, *Student Member, IEEE,* Wanchun Dou, *Member, IEEE,* Shui Yu, *Senior Member, IEEE,n*and Zhensheng Zhang, *Senior Member, IEEE "*A Decentralized Cloud Firewall Framework withResources Provisioning Cost Optimization" publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.IEEE Transactions on Parallel and Distributed Systems in 2014

[2] Hongxin Hu, Student Member, IEEE,Gail-Joon Ahn, Senior Member, IEEE,"Detecting and Resolving Firewall Policy Anomalies" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 3, MAY/JUNE 2012

[3] Security Guidance for critical areas of focus in cloud computing vol 3.0 by Cloud Security Aliance

[4] Deyan Chen1,Hong 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

[5] Wentao Liu, "Research on Cloud Computing" published in 2012 IEEE

[6] Sivadon Chaisiri, Student Member, IEEE,Bu-Sung Lee, Member, IEEE, and Dusit Niyato, IEEE, "Optimization of Resource Provisioning Cost in Cloud Computing" published in IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012

[7] Yi-Ju Chiang, Student Member, IEEE, Yen-Chieh Ouyang*, Member, IEEE, and Ching-Hsien Hsu, Senior Member, IEEE, "An Efficient Green Control Algorithm in Cloud Computing for Cost Optimization " IEEE TRANSACTIONS ON CLOUD COMPUTING, TCCSI-2014-03-0116

[8] Ren-Hung Hwang1, Chung-Nan Lee2, Yi-Ru Chen1, Da-Jing Zhang-Jian2, "Cost Optimization of Elasticity Cloud Resource Subscription Policy" IEEE TRANSACTIONS ON JOURNAL NAME 1939-1374/2013 IEEE

[9] Balaji Palanisamy, *Member, "*Cost-effective Resource Provisioning for MapReduce in a Cloud*"published in* IEEE Transactions on Parallel and Distributed Systems 2013 IEEE.

[10] Keke Chen, James Powers, Shumin Guo, and Fengguang Tian, "CRESP: Towards Optimal Resource Provisioning for MapReduce Computing in Public Clouds" published in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 6, JUNE 2014

[11] Edward G. Amoroso, AT&T,"Practical Methods for Securing the Cloud" IEEE Cloud Computing published by the IEEE computer society 2014 IEEE

[12] Mohamed Abu Sharkh, Manar Jammal, Abdallah Shami, and Abdelkader Ouda, Western University, "Resource Allocation in a Network-Based Cloud Computing Environment: Design Challenges" IEEE Communications Magazine • November 2013

[13] Melanie Posey September 2014," WHITE PAPER Journey to the Hybrid Cloud" published in September 2014, IDC #242798R1