Mathematical Statistician and Engineering Applications
ISSN: 2326-9865
DOI: https://doi.org/10.17762/msea.v70i1.2296

A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization

Prateek Srivastava

Associate Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number: 164-172
Publication Issue:
Vol. 70 No. 1 (2021)

Article History
Article Received: 25 January 2021
Revised: 24 February 2021
Accepted: 15 March 2021

Abstract
A new flexible method for supplying more computer power in a shared media is called cloud computing. It offers a distributed paradigm based on self-evaluation methods to increase the system's processing power with less managerial worries. Clients, applications, platforms, servers, and infrastructures make up its components. This computing architecture provides end users with calculation skills as a computed service from the aforementioned components. Security management will lose importance when more devices and their integration become available. One needs to manage data, system, and confidentiality problems carefully since cloud users are growing daily. Therefore, in order to address protected access and integrity concerns in a cloud environment, new security firewall services must be deployed in addition to the current system. Numerous network-related issues, including load balancing, scheduling, traffic divergence, filtering, regulating the rate of arrival, instance management, and attack detection, make it difficult to implement firewalls for cloud computing. A centralised cloud firewall makes it very difficult to predict the response time. Consequently, a new line of work has been established for actually implementing the new firewall techniques for the cloud. In order to reduce the cost of ownership and operation, it also strives to achieve resource optimization-based provisions and guidelines.

Keywords: Cloud Computing, Self-Evaluation Method, Security Management, Firewall Framework.

1. Introduction

With the quick advancement of computer hardware and software, cloud computing has emerged as a major problem in business and academics. The conventional computer and communication technologies, as well as commercial practises in the sector, are only a few of the elements that have led to the development of cloud computing. Completely network-based and designed with the customer in mind. The user receives a service from the cloud computing system, which is very scalable and reliable. The user is unaware of the location of the resource since it is transparent to the programme in the cloud system. Your apps and data are accessible to users from any location. A huge number of users can share resources in cloud computing platforms. The growth of information technology for the benefit of society will be further impacted by the cloud computing system, which is a significant transformation in the information sector. It comprises of dependable services provided by data centres constructed on servers using varying degrees of virtualization technologies and methods. Since the cloud computing system can provide data security and users won't need to take additional steps to

secure their data, the safety of data kept in a cloud computing system must be guaranteed. The cloud computing platform is offered by many businesses, like Google, IBM, and Microsoft, although it has to be safeguarded more thoroughly than a conventional system. Other individuals who are not a member of the firm can view the data.

The most significant issue preventing the growth of cloud computing is security. Data security, client data security assurance, dependability of the cloud computing platform, and cloud computing organisation are the primary security concerns. Because the cloud system is based on the internet, it has many of the same security flaws as the internet. The biggest concerns with cloud computing are security including protection, including common security problems like infection, hacking, and security flaws can also pose risks to the cloud system. A development in virtualization, administration-focused structural planning, and utility computing through the Internet is cloud computing. Applications, platforms, and administrations are all part of it, but it's crucial to make sure the resource is safe. The customer cannot regulate how the data is handled moving forward and confirm the security of the data since cloud services hide the specifics of administrative execution and management. The cloud system may store the data in several cloud nodes and distribute the cloud focus over a wide area. The security management has to be improved to handle the legal risk.

In order to protect against unauthorised access to Internet-based businesses and suspicious traffic, firewalls are crucial components of network and data system security. For setting up a security policy in a firewall, system administrators build a set of filtering rules that are derived from the hierarchical network security necessities. As a result of the difficulty as well as dependency of policy rules, managing firewall policies is a difficult process that is made even more difficult by the ongoing evolution of network and system environments. For instance, despite the fact that multiple specialists maintained their firewall policies, some administrators claimed that the policies include abnormalities. Wool recently examined firewall policies gathered from several organisations and found security issues in every single one of them. Given that a firewall policy may have a sizable number of rules that are frequently conceptually intertwined with one another, the number of conflicts in a firewall has the potential to be significant. Conflicts between policies are frequently quite complex; one policy may clash with several distinct rules, and one conflict may be related to several other regulations. A network's firewall policies are frequently updated by several managers, and an enterprise firewall may have historical rules created by various administrators. A firewall often uses a first-match resolution technique that relies on the sequence of rules to resolve policy conflicts. Each packet the firewall processes is mapped to the first judgement that the packet matches in order to identify policy conflicts. There are limitations to using the first-match technique to resolve policy disputes, too.

In order to enable more precise anomaly identification and efficient anomaly resolution, this study introduces an innovative firewall anomaly management approach that utilizes rule-based segmentation. The cloud model's current flaws will also make hackers more dangerous. By developing a stochastic programming model, an optimum cloud resource provisioning (OCRP) method is put forth as a solution to this issue. The OCRP algorithm may allocate computer resources for a long-term plan and several provisioning phases, such as four stages in a

quarterly plan and twelve stages in an annual plan. Numerous numerical experiments have been conducted, and the findings show that cloud consumers may successfully minimise the overall cost of resource provisioning in cloud computing environments by using the OCRP algorithm.

Additional considerations were the impact of VM re-configuration delay and the restriction on the minimum rental duration for VM startup. This article introduces Cura, a brand-new MapReduce cloud service paradigm for data analytics. It contends that current cloud services are insufficient and wasteful for production workloads and that industrial and governmental entities are paying more attention to energy consumption. Algorithms for resource allocation are used to assign virtual machines on servers located in data centres and network resources while adhering to the limitations of the problem. To serve as a guide for creating a thorough energy-aware resource allocation model for cloud computing data, design problems are highlighted.

2. Literature Survey

With the use of virtual private network (VPN) technology, mobile users may safely access a remote computer on the open Internet as if it were a device connected to their company's network. We suggest VGuard as a solution to this problem, a framework that enables a policy owner as well as a request owner to jointly decide if a request fulfils a policy without the policy owner and request owner knowing each other's policies. The Cross-Domain Cooperative Firewall (CDCF) framework is far inferior to VGuard, which is not only considerably more efficient but also significantly more secure. The core issue in this application is how to cooperatively enforce firewall rules for VPN tunnels in an open distributed environment while protecting user privacy. The three criteria of policy privacy, request privacy, and protocol efficiency should all be satisfied by a workable solution. Despite any number of protocol executions, the policy owner is unable to discover more about the policy than they would by using brute force probing. For distributed applications, prompt processing of each request (or packet) is essential, and the overhead of the solution should be minimal [1].

This study proposes a methodology for evaluating the effectiveness of various firewall platforms. Measurements including latency, jitter, throughput, and packet loss are taken into account in the study. Real-world tests of the suggested evaluation technique are undertaken on various firewall kinds, and a quantitative analysis is carried out to investigate the degree of knowledge among the educated group in the community. Network-based and personal firewalls are the two basic types. Personal firewalls are placed on personal devices, whereas network-based firewalls are put at the network's edge. This study proposes a methodology for evaluating the effectiveness of various firewall platforms. It takes into account packet loss, jitter, throughput, and delay. Applying a series of assaults and monitoring the firewalls' responses is another way to assess the security of firewalls. Examining a sample of college students' degree of understanding on the significance of firewalls and how to use them is a secondary goal. Personal and network-based firewalls are the two types of firewalls. Host packet filtering is a function of personal firewalls that aims to defend individual hosts from harmful transmissions [2].

ISSN: 2326-9865
DOI: https://doi.org/10.17762/msea.v70i1.2296

This article suggests a firewall outsourcing strategy that protects privacy by having companies hire ISPs to handle their firewall needs without disclosing their firewall policies. The fundamental concept is that organisations anonymize their firewall policies before sending them to their ISP, who subsequently filters packets in accordance with the anonymized regulations. The firewall throughput of the scheme operating at ISPs is equivalent to that of software firewalls operating at enterprises themselves, according to experimental results, which also demonstrate that the system is efficient in terms of memory use and packet search time. Businesses start outsourcing their firewall services to ISPs to cut administration and implementation expenses. Network-Based Firewall Services (NBFWS), which AT&T has begun selling, can help organisations save money in terms of maintenance, implementation, and upgrading. According to this paradigm, businesses must provide their ISP with their firewall policy so that the ISP may filter the incoming and outgoing traffic of the business according to that policy. Due to the present firewall outsourcing model, which mandates that companies disclose their firewall policies to their ISPs, the privacy problem of firewall policies has, nevertheless, become a real worry [3].

A new flexible method for supplying more computer power in a shared media is called cloud computing. It offers a distributed paradigm based on self-evaluation methods to increase the system's processing power with less managerial worries. It consists of a client, an application, a platform, servers, and infrastructures, and it gives consumers the ability to compute as a calculated service using the aforementioned components. In order to address protected access along with integrity concerns in a cloud environment, security firewall services must be introduced. The user receives a service from the cloud computing system, which is very scalable and reliable. A huge number of users can share resources in cloud computing platforms. Because it offers a single point of access for all computing requirements, cloud computing represents a significant transformation for the information sector. The cloud computing platform is offered by businesses including Google, IBM, Microsoft, Amazon, VMware, and EMC. Data that is kept in the cloud system shouldn't be deleted or taken since other people could be able to see it. For computing to take place on the cloud service provider's infrastructure, governance and security are crucial [4].

DDoS assaults are a sort of cyberattack that aims to deplete the victims' computational, network, and operating system data structures resources. Early cyberattacks were mostly carried out for entertainment and curiosity, but more recently, attacks have increased as a result of the enormous financial or political benefits accessible to cybercriminals. Major DDoS assaults, which may take many different forms, like flooding packets or synchronisation attacks, are powered by botnets. To counter flash crowd imitation assaults, a similarity-based DDoS detection technique has been suggested. Increasing resource investment is a passive defence tactic, but doing so is expensive because most of the increased resources are sitting idle. Resource management and cooperation are essential to DDoS mitigation solutions for non-cloud systems. The implementation of a router throttle was suggested by Yau et al. to limit the volume of attack packets travelling far from the protected server. Using a divide-and-conquer tactic, Chen et al. devised the attack diagnostic (AD) DDoS assault mitigation technique. He et al. investigated the bandwidth-latency tradeoff for task migration in a cloud

environment, while Wang et al. examined the optimal resource allocation problem on the cloud platform offered by the customer, Spot Cloud [5].

3. Proposed System

Despite the many benefits of cloud computing, there are still a lot of practical issues that need to be resolved. The market size for public and hybrid clouds is $59 billion, and it will increase to USD 149 billion by with a compound annual growth rate of 14%, according to a Gartner study on cloud computing revenues. The revenue projection suggests that the cloud computing sector is a promising one. However, from a different angle, the cloud model's current security flaws will make hackers more dangerous. Data security and privacy protection concerns are the main challenges that need to be handled as soon as possible, corresponding to service delivery models, deployment patterns, as well as fundamental elements of cloud computing. Issues with data security and privacy can be found at all levels of SPI service delivery models as well as across the whole data life cycle. Sharing data while preserving personal information presents difficulties for privacy protection. E-commerce systems that hold credit cards and healthcare systems with patient data are the usual systems that need privacy protection. Controlling what information to share and who may access it online has become an increasingly important topic. Sensitive data must be kept strictly separate from non-sensitive data in the cloud environment, and then sensitive parts must be encrypted. Two computing resource provisioning options, referred to as reservation and on-demand plans, are available to cloud service providers to offer to their customers.

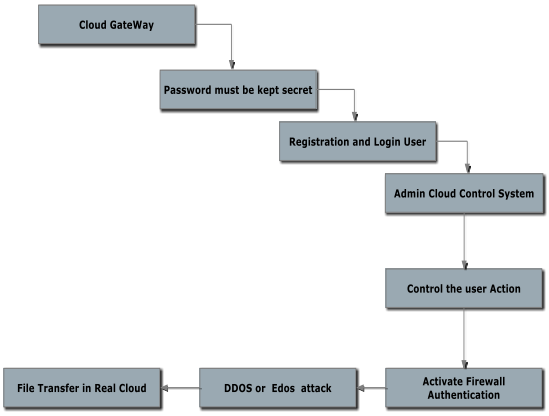

Fig 1: System Architecture

Cost of using computer resources provided through reservation, in general. This issue is addressed by developing an optimum cloud resource provisioning (OCRP) method using a stochastic programming paradigm. The OCRP algorithm may allocate computer resources for usage in a long-term plan as well as many provisioning phases, such as four provisioning stages for a quarter plan and twelve stages for an annual plan. In OCRP, the demand as well as cost uncertainty are taken into account. The OCRP algorithm's solution is sought using a variety of methods, including Benders decomposition, sample-average approximation, and deterministic equivalent formulation. Numerous numerical experiments have been conducted, and the

findings prove it unequivocally that the OCRP algorithm enables cloud consumers to successfully reduce the overall cost of resource procurement in cloud computing environments.

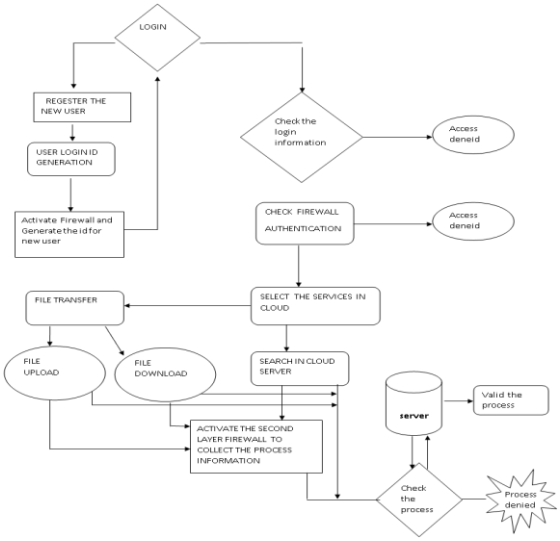

Fig 2: Flow Diagram

IaaS infrastructure has recently gained popularity as a platform for application developers to distribute their apps. IaaS companies, however, give a variety of VM configurations and charge various prices for them. They also provide a variety of pricing structures. The ideal technique to efficiently provide or subscribe VM resources from an IaaS provider is brought up as an intriguing question for application providers. In this study, the resource provisioning problem was defined as a two-phase resource planning issue. The best long-term resource provisioning was the main goal of the first phase.

In order to determine the best long-term resource design and reduce anticipated operational costs, we put out certain mathematical equations. For estimating resource demand, we put up a Kalman filter prediction model in the second phase. As an Integer Programming issue, after that, converted the ideal resource configuration for the anticipated demand into an Unbounded Two-Dimensional Knapsack issue, which may be resolved using dynamic programming or heuristic techniques. In our study, we also took into account a number of other difficulties, such as the impact of VM re-configuration delay and the restriction on the minimum rental duration for VM startup. Based on workload information from an actual system and the Amazon EC2 pricing model, we assessed our suggested solutions.

Our numerical findings demonstrated that the suggested long-term resource planning method had the potential to provide operating costs that were almost ideal. The outcomes also shown that the suggested on-demand planning algorithm has the ability to handle the delay of VM reconfiguration and greatly lowered operating costs. For each individual cloud client, the proposed solution offers a decentralised cloud firewall structure.Response times via each firewall can meet the QoS criterion by dividing the packet arrival rate among numerous parallel fire-walls and starting the appropriate VM instance for each firewall.The system establishes a mathematical model in accordance with the cloud firewall rule matching discipline therefore concludes that system service times follow a geometric distribution.The maximum number of

ISSN: 2326-9865
DOI: https://doi.org/10.17762/msea.v70i1.2296

concurrent VM instances that may be used by an account is often limited by CSPs. The following benefits of the suggested strategy are listed:

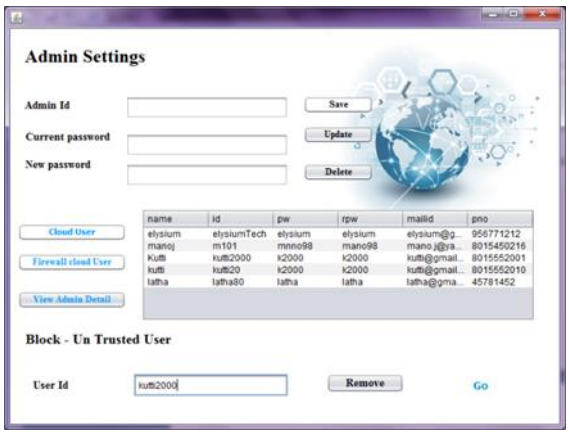

Fig 3: Untrusted User Blocked by Admin

- Resources are dynamically assigned to reduce provisioning costs and simultaneously ensure that customers' requested QoS is met.
- According to the simulation results, modelling firewall systems is more suited for geometric distribution.
- It provides a thorough understanding of the tradeoffs between optimal resource provisioning costs.
- The system calculates the cost of supplying resources.

4. Results

Although security is always a worry, cloud computing provides a flexible way to deliver more processing power on a shared media. A new path has been set in order to accomplish new firewall tactics and resource-based provisions and regulations in order to solve this. To reduce the overall cost of resource providing in cloud computing settings, an optimum cloud resource provisioning (OCRP) method is presented. It is suggested to use a Kalman filter prediction model to forecast resource demand and create the ideal resource configuration. To conserve local discriminative information and maximise the information offered by each bit to learn compact hashing codes, a novel hashing approach is presented. The accompanying pictures show how extensive tests on four datasets revealed advantages over alternative approaches.

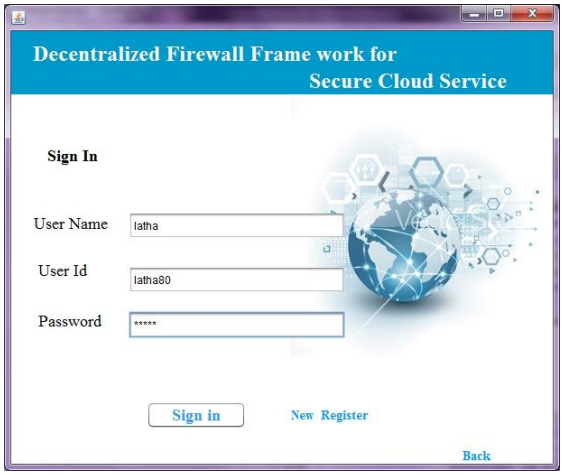

Fig 4: User Login

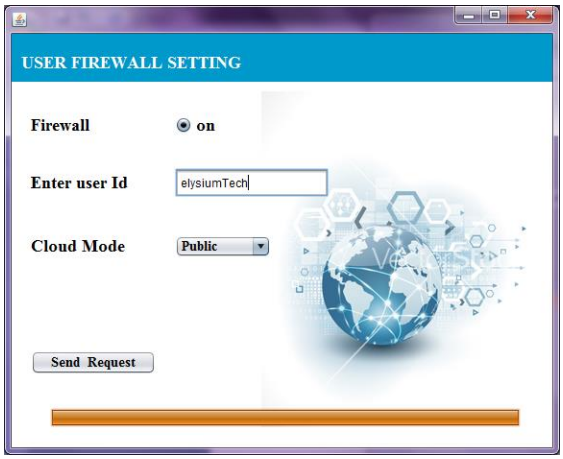

Fig 5: Firewall Activation

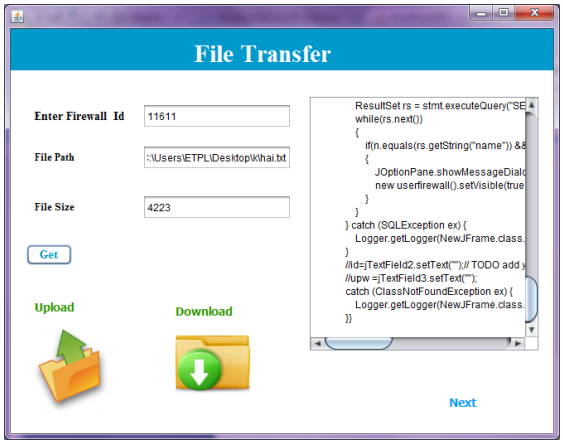

Fig 6: File Transfer

5. Conclusion

By maintaining the local discriminative information for picture indexing, we suggest a unique hashing algorithm in this study. The suggested technique seeks to maintain the local discriminative information following binarization, which is different from the prior hashing

algorithms. That is, from the neighbour samples a sample chooses in the original space, the labels of the sample may be accurately predicted in the Hamming space. In the meanwhile, the suggested technique maximises the information offered by each bit and reduces duplication in the learnt hashing bits as much as feasible in order to learn compact hashing codes. Our approach is capable of teaching discriminative and small hashing codes. On four datasets for picture retrieval that are openly available, extensive experiments are conducted. The comparative findings have demonstrated how much better our methodology is than many other approaches.

Reference

1. L. Parfeni, “Flickr boasts 6 billionphoto uploads,” Softpedia, Tech. Rep., Aug. 2011.
2. A. Jeffries, “The man behind Flickr on making the service ‘awesome again,”’ The Verge, Tech. Rep., Mar. 2013.
3. B. Kulis, P. Jain, and K. Grauman, “Fast similarity search for learned metrics,”IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 12, pp. 2143–2157, Dec. 2009.
4. Z. Li, J. Liu, J. Tang, and H. Lu, “Robust structured subspace learning for data representation,” IEEE Trans. Pattern Anal. Mach. Intell., Feb. 2015, doi: 10.1109/TPAMI.2015.2400461.
5. S. Meiser, “Point location in arrangements of hyperplanes,”Inf. Comput., vol. 106, no. 2, pp. 286–303, 1993.
6. A. Andoni, “Nearest neighbor search: The old, the new, and the impossible,” Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2009. TANGet al.: NDH FOR LARGE-SCALE IMAGE RETRIEVAL 2839
7. J. Wang, J. Wang, N. Yu, and S. Li, “Order preserving hashing for approximate nearest neighbor search,” in Proc. ACM Int. Conf. Multimedia, 2013, pp. 133–142.
8. A. Torralba, R. Fergus, and Y. Weiss, “Small codes and large image databases for recognition,” inProc. IEEE Int. Conf. Comput. Vis. Pattern Recognit., Jun. 2008, pp. 1–8.
9. W. Liu, J. Wang, R. Ji, Y.-G. Jiang, and S.-F. Chang, “Supervised hashing with kernels,” inProc. IEEE Int. Conf. Comput. Vis. Pattern Recognit., Jun. 2012, pp. 2074–2081.
10. P. Indyk and R. Motwani, “Approximate nearest neighbors: Towards removing the curse of dimensionality,” in Proc. ACM Symp. Theory Comput., 1998, pp. 604–613.
11. Y. Weiss, A. Torralba, and R. Fergus, “Spectral hashing,” in Proc. Adv. Neural Inf. Process. Syst., 2008, pp. 1753–1760.
12. R. Salakhutdinov and G. Hinton, “Semantic hashing,”Int. J. Approx. Reasoning, vol. 50, no. 7, pp. 969–978, 2009.
13. B. Kulis and K. Grauman, “Kernelized locality-sensitive hashing for scalable image search,” in Proc. IEEE 12th Int. Conf. Comput. Vis.,Sep./Oct. 2009, pp. 2130–2137.
14. W. Liu, J. Wang, S. Kumar, and S.-F. Chang, “Hashing with graphs,” in Proc. Int. Conf. Mach. Learn., 2011, pp. 1–8.
15. J. Wang, S. Kumar, and S.-F. Chang, “Semi-supervised hashing for large scale search,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 12,pp. 2393–2406, Dec. 2012.
16. X. Li, G. Lin, C. Shen, A. van den Hengel, and A. Dick, “Learning hashing functions using column generation,” inProc. Int. Conf. Mach. Learn., 2013, pp. 142–150.