Monitoring Performances of Quality of Service in Cloud with System of Systems

Helen Anderson Akpan[1], M. R. Sudha[2]
[1]MSc Student, Department of Information Technology,[2]Assistant Professor, Department of Computer Science, SRM University, Tamil Nadu, India.
[1]helen_anderson@srmuniv.edu.in
[2]sudha.mr@ktr.srmuniv.ac.in

Abstract: Currently, cloud computing plays a major role in the delivery of Information Technology (IT) resources via the internet in an on-demand fashion to enterprise systems and other cloud users. Service providers and operation centers encounter a lot of challenges as cloud services such as software as service, platform as a service and infrastructure as a service are being utilized by the end users. Monitoring the performances of quality of service (QoS) is daunting as such service providers and data centers have challenges in dealing with the QoS related issues. There is a necessity to monitor the various layers of cloud computing environment to provide an end-to-end solution for QoS problems. This project is an extension of a previous work that was carried out to ascertain the efficiency of the QoS techniques employed in existing systems. In this paper, we explore the System of Systems (SoS) approach and attempt to present a viable solution to ensure effective QoS performance monitoring in the cloud environment. The deliverable of the project is an online transaction application which can monitor and manage the performances of Quality of Service in the cloud environment. Furthermore, cryptographic technique is employed for security purpose and distributed denial of service (DDOS) solution is also presented.

Keywords: Cloud Computing, Distributed Denial of Service (DDoS), Quality of Service (QoS), Security

I. INTRODUCTION

Cloud computing has the potential for tremendous benefits, but wide scale adoption has a range of challenges in terms of quality of service which has to be addressed [1]. With Cloud computing, users can share enormous volume of data at high speeds over the internet at reduced cost irrespective of their geographical location. Cloud Service Providers provide services namely, Infrastructure as a Service (IaaS), Platform as a service, Software as a Service (SaaS), Business as a Service (BaaS) and Governance as a Service (GaaS) to the end users. These services are leased according to a usage-based pricing model. As more consumers delegate their tasks to cloud providers, Service Level Agreement (SLA) between the consumers and providers becomes a necessity. Due to the dynamic nature of the cloud, continuous monitoring of the QoS attributes is also necessary to enforce SLA. Again, other factors such as security, performance and reliability have to be considered particularly for enterprise consumers that may outsource its critical data [2].

Furthermore, a System of Systems (SoS) approach to provide a clear and concise view of QoS events within cloud computing environment that proactively informs the enterprise operators of the state of the enterprise and enable timely operators response to QoS problems is required [3]. From the inference of the survey [4] carried out to ascertain the extent of work done to resolve QoS challenges, the existing techniques and approaches need to be enhanced to handle these challenges effectively. The deliverable of this project is an integrated Software as a Service (SaaS) via online transaction application which enables monitoring performances of quality of service in the cloud environment using System of Systems approach. Security metrics are considered and encryption technique is used to provide server side security to the users. Again, security measures are taken to prevent distributed denial of service (DDoS) attacks in the cloud environment.

II. LITERATURE REVIEW

In recent years, numerous research works on QoS in cloud environment have been carried out. Researchers in their quest for an efficient solution for QoS problems have formulated a lot of models, designed framework, employed algorithms and feasible techniques to improve QoS in the cloud environment.

P. C. Hershey et al [3] explored the issue of QoS observation and response time in the cloud environment using a System of Systems approach. The approach employed was enterprise monitoring, management and response architecture for cloud computing (EMMRA CC). The approach extended previous work to provide structure from which to identify points within the administrative domain, where QoS metrics may be monitored and managed. Simulated results were used to confirm the efficacy of the approach. Though an excellent approach was used and accurate results were obtained, no implementation has been carried out in real time or in federated cloud.

M. Salama et al. [5] presented a QoS-oriented federated cloud computing framework where multiple independent cloud providers can cooperate seamlessly to acquire more resources in peak time to fulfill their QoS targets and pre-define SLAs new QoS levels in terms of their scaled resources after performing federation agreements. The framework includes formalization of federated agreements, workload prediction and QoS continuous evaluation, besides resource monitoring and allocation. The framework offers QoS-oriented capabilities to address dynamic resource management, aiming to dramatically improve the effective usage resources.

W. E. Dong et al. [6] presented a paper which focused on QoS oriented cloud computing resources availability. A monitoring model of cloud computing resource availability was developed. Based on the dynamic process of cloud computing service, availability of cloud computing resources was analyzed from QoS of a single cloud resource node which is described by common attribution and special attribution to QoS of some cloud resources which are connected by series model, parallel model; and mix model to provide service. In this paper, a QoS model which can be configured dynamically to describe the QoS of resources in cloud computing was introduced. A local optimization algorithm mathematical model was designed to solve the resource selection problem.

X. Zheng et al. [7] took a service perspective and initiated a quality model named CLOUDQUAL for cloud services. It is a model with quality dimensions and metrics that targets general cloud services. To demonstrate the effectiveness of CLOUDQUAL, empirical case studies on three storage clouds were conducted. Results showed that CLOUDQUAL can evaluate their quality. CLOUDQUAL was validated with standard criteria to show that it can differentiate service quality.

S. Lee at al. [8] proposed an architecture which employed the agent technology to handle the monitoring of QoS requirements and service level agreements which support verification, validation and can dynamically analyze resources allocation and deployment. A middleware was designed for enterprise cloud computing which can automatically manage the resource allocation of services from platforms and infrastructures and provide a cost-effective and secure way to access services from cloud environment.

G. Cicotti et al. [9] presented QoSMoNaaS (Quality of Service Monitoring as a Service), a QoS monitoring facility built on top of the SRT-15, a cloud oriented and CEP-based platform being developed in the context of the homonymous European Union (EU) funded project. In particular, the main components of QoSMoNaaS were presented and QoSMoNaaS operation and internals with respect to a substantial case study of an internet of things (IoT) application was illustrated.

M. J. Dimario et al. [10] discussed a constitutive SoS framework with regard to the new behavior that emerged as a result of a mechanism of collaboration that architected to affect a holistic capability among autonomous systems. The approach was actualized with a case study that revealed that the performance of autonomous collaboration as a SoS exhibits greater capability than the autonomous units performing independently.

P. C. Hershey et al. [11] presented a paper that extended previous work on end-to-end enterprise monitoring to address the additional monitoring challenges imposed by SOA based net-centric system for which enterprise resources are made available as independent services that can be accessed without knowledge of their underlying platform implementation. They presented a novel approach for SOA monitoring applied to enterprise computing systems. Metrics for SOA monitoring were presented along with an SOA monitoring framework and reference monitoring architecture.

P. C. Hershey et al. [12] presented a detailed procedure for identifying both the on-set of DDoS attack and the corresponding counter measures to prevent or limit their effects. The procedure was used to detect and respond to DDoS attacks on complex enterprise systems thus overcoming the limitations of the previous techniques. The procedures employed mitigation steps to proactively counter various attacks, regardless of the SOA layer in which they were detected and trace back capabilities that enable operators and analysts to proactively locate and negate the attacks identified.

S. S. Chopade et al. [13] presented a simple distance estimation based technique to detect and prevent the cloud from flooding based DDoS attack and thereby protect other servers and users from its adverse effects. In this technique the mean value of distance in the next time period was estimated using the exponential smoothing estimation technique. The proposed technique relied on MMSE to support efficient traffic arrival rate prediction for separated traffic. The technique was tested in the internet-like network implemented on NS2 with over 100 nodes. The experimental results showed that the proposed technique was effective and can detect DDoS attacks with high detection rate and false positive rate.

III. METHODOLOGY

In this work, QoS issues are solved for the cloud environment. We constructed ‘n’ number of nodes so that the nodes can communicate with each other in the network. The cloud server, in this case Google drive was used to store all files and file details while the database was used to store the nodes information. In the Google drive we demonstrated the concept of SoS, we created different repositories to serve as different cloud servers for easier and more efficient access to cloud services.

We divided the project into six modules: authentication, service request, user verification and security check, route selection, data transmission, and performance analysis. The performances of QoS metrics such a throughput, response time and delay were monitored in the administrative domain. We defined Throughput as how much data is transmitted in a given interval of time. Given by: T = n * t

Where, T is throughput, n is the number of data transmitted, and t is time in seconds.

We calculated the response time as the work time, i.e. the time difference for each transaction. Given by: Rt = wt

Where Rt is response time, and wt is the work time in seconds.

We defined delay as the time difference between the file size and file time converted to kilo bytes. Given by: Tdif = filesize - filetime

Where Tdif is the time difference, filetime = workdur * 1024 * 1024, (workdur is the work duration and filetime is converted to kilo bytes).

The system architecture and Activity diagram is given in fig.1 and fig. 2 respectively.

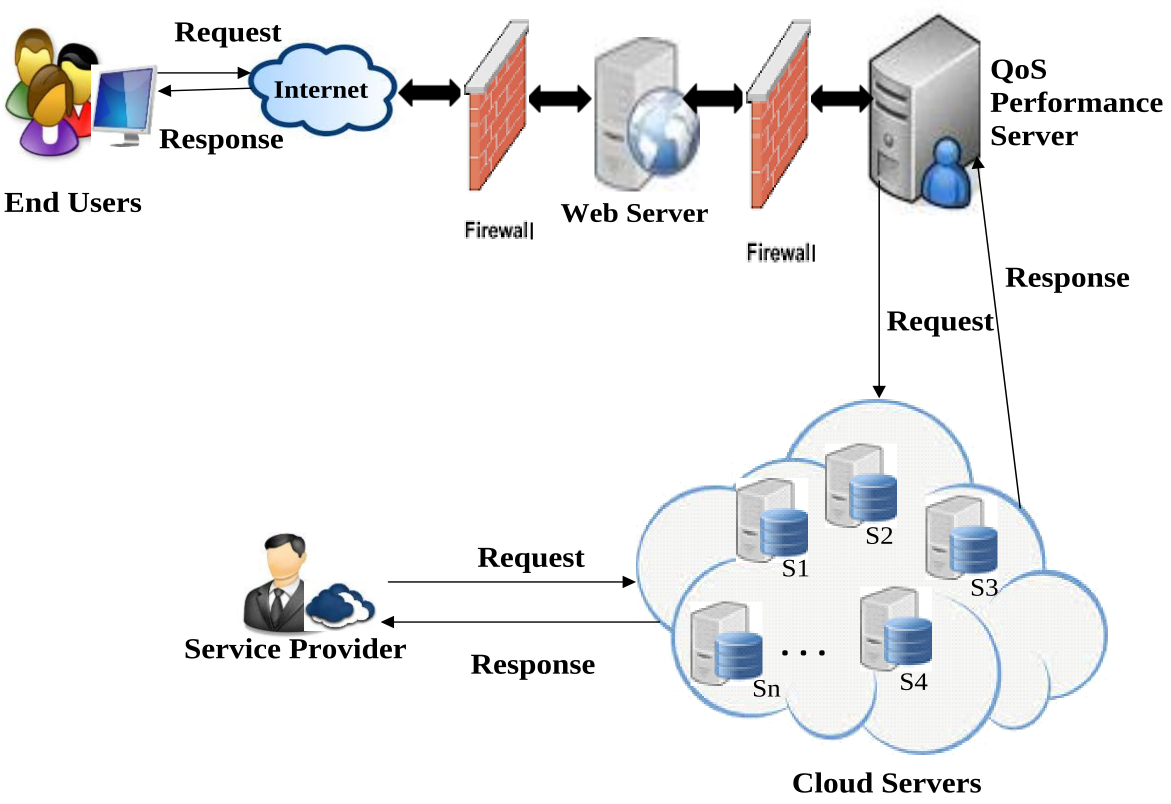

Fig 1: System Architecture

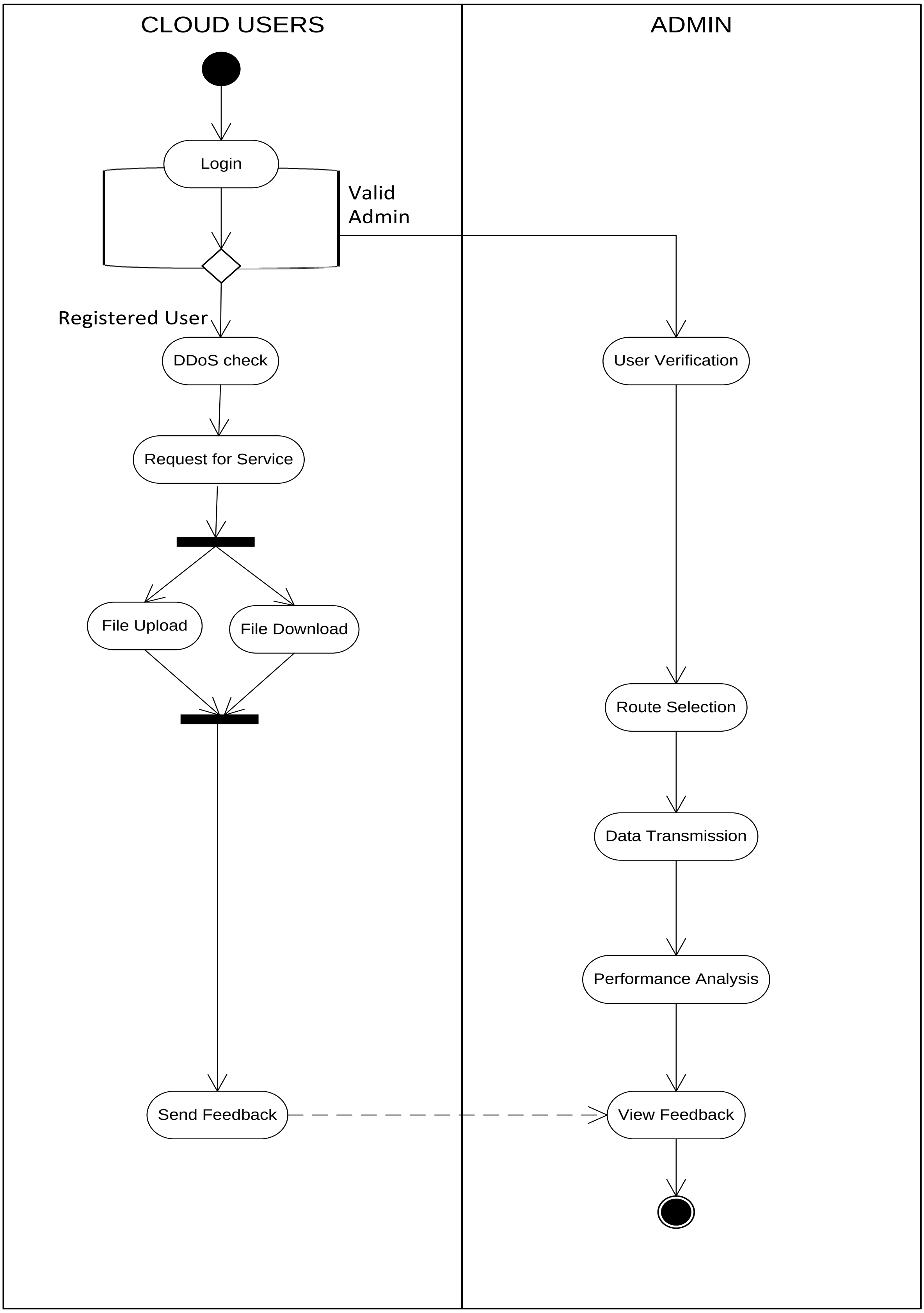

Fig. 2: Activity Diagram

IV. RESULTS AND DISCUSSION

We developed an online transaction application and integrated Google drive into the application. Instead of carrying out simulation experiment, we employed Google drive to demonstrate the SoS approach. We created separate repositories in Google drive to serve as cloud servers and uploaded and downloaded files based on the specification of the various repositories. We categorized the folder according to the type and size of file requested. The categorization was useful in minimizing queue and reducing the delay time of uploading or downloading file from the destination node or neighboring node based on resource availability.

We employed route selection strategy, such that the application is able to select an appropriate source node to download from or destination to upload to, depending on the type of resource requested. In our sample online processing application, the response time, delay and throughput is calculated for each request and response respectively. The QoS metrics such as response time, delay and throughput are monitored in the administrative domain in order to improve QoS in the cloud environment. Encryption technique was used to maintain the integrity of users' data while security measures were taken to track the user's IP address in order to prevent DDoS attacks. Results verified that the SoS approach can significantly improve the Quality of Service in the cloud environment.

A. Delay, Response time and Throughput Performance Metrics Verification

Performance metrics were measured & recorded at diverse time granularities using an online transaction processing application.

Assumptions

QoS thresholds can be changed for different application scenarios (i.e., need not be fixed a priori for all applications to be deployed on a cloud).

Observations

Both Variation in Delay over time and Throughput are indicators of the overall system performance.

Actions

(i) QoS thresholds were fixed (e.g., throughput per hour and delay per second) for the application scenario to be verified.

(ii) Prototype transaction processing application monitored service domains for QoS breach.

(iii) If a QoS breach was observed, then a response action (RA) (i.e., an automated action to rectify the breach) was initiated automatically.

B. Summary of Results for Performance of QoS metrics

We analyzed the performances of QoS metrics during upload and download of ten sample files. We obtained the following results for hourly time periods.

TABLE 1: Summary of Results for Performance of QoS Metrics

Time Period	Delay Time (seconds)	Throughput (no of transactions)
10:00:00-11:00:00	7	50
11:00:00-12:00:00	5	55
12:00:00-13:00:00	6	53
13:00:00-14:00:00	8	50
14:00:00-15:00:00	4	59
15:00:00-16:00:00	7	52
16:00:00-17:00:00	6	53
17:00:00-18:00:00	3	60
18:00:00-19:00:00	5	57
19:00:00-20:00:00	5	54

(i) Throughput

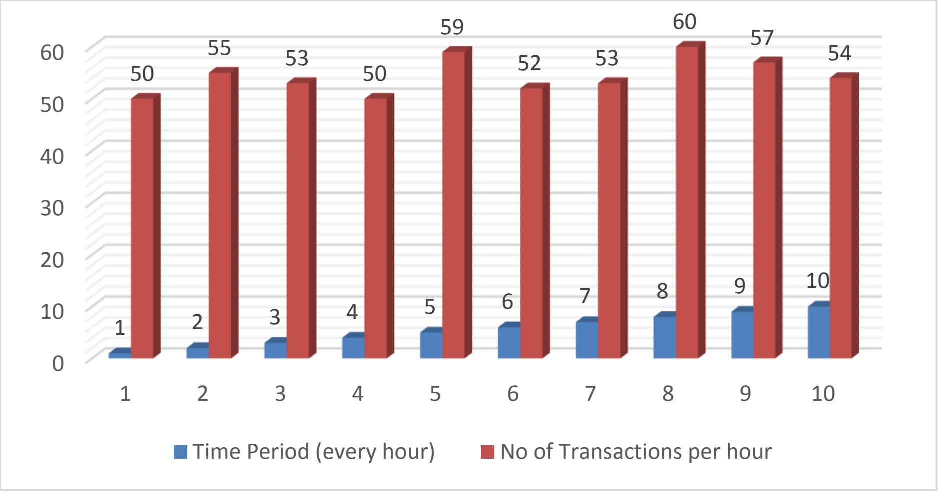

Fig. 3: Throughput

We calculated the throughput based on the total number of transactions per specified time period. We noticed that the throughput varied depending on the file size and file type of the uploaded and downloaded file. The result obtained indicated significant high performance.

(ii) Delay

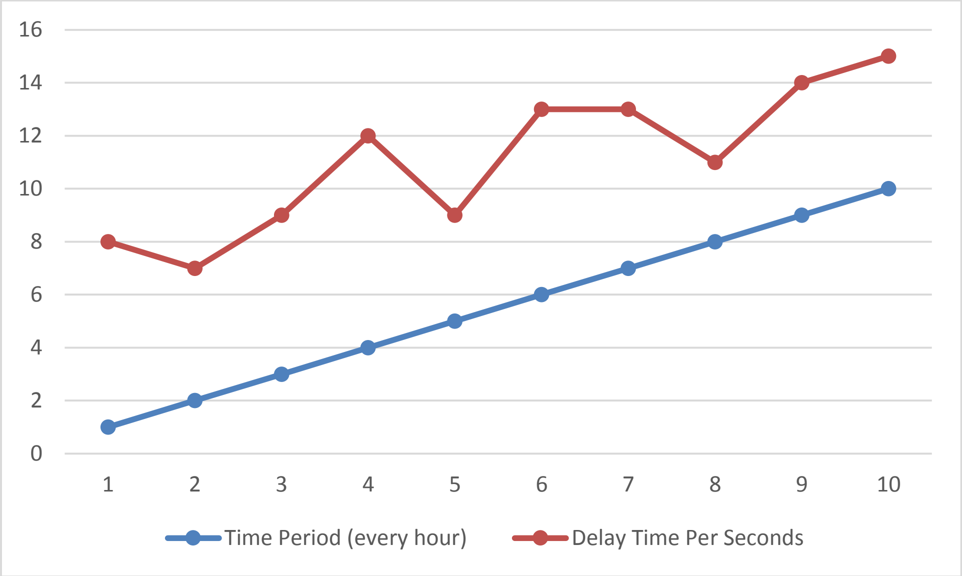

Fig.4: Delay

In Fig.4, the delay for each transaction was computed. We observed that there was minimal delay during the transactions, and the delay varied depending on the type and size of application uploaded or downloaded. The online transaction application was developed to possibly eliminate delays in order to improve the QoS in the cloud environment.

C. Security

The following security measures were implemented to eliminate security threats in the cloud environment.

(i) Cryptographic technique was used to encrypt the cloud users' details in the application level.

(ii) Users' verification was carried out at the administrative domain for authorization.

(iii) We tracked the IP address of the users at the application level in order to detect DDoS Attackers and prevent security threats.

V. CONCLUSION

In this paper, we presented a solution for QoS issues in cloud environment. We employed Google drive as cloud server for our online transaction application and created different repositories to demonstrate the SoS approach. We monitored the performances of QoS within the administrative domain during downloading and uploading into Google drive as per the cloud users' request. Cryptographic technique was used to encrypt users' data and measures were also taken to prevent DDoS attacks. In future, we intend to liaise with the cloud service providers and integrate their servers into our application instead of using Google drive. The cloud users will be able to access and make use of cloud services from various service providers while the performances of QoS will be monitored within the administrative domain in real time.

REFERENCES

[1] C. A. Lee, "A perspective on scientific cloud computing", in Proc. ACM Int. Symposium on high performance distributed computing, pp. 451-456, 2010.

[2] P. Patel, A. H. Ranababu, A. P. Sheth, "Service level agreement in cloud computing", Kno.e.sis publications, pp. 1-3, 2009.

[3] P. C. Hershey, S. Rao, C. B. Silio, A. Narayan, "System of systems for quality-of-service observation and response in cloud computing environment", IEEE Systems Journal, Volume: 9, Issue: 1, pp. 1-5, 2015.

[4] A. A. Helen and V. B. Rebeccajeya, "A survey on Quality of service in cloud computing", International Journal of Computer Trends and Technology (IJCTT), Volume: 27 Number: 1, pp. 58-63, 2015.

[5] M. Salam and A. Shawish, "A QoS-oriented inter-cloud federation framework", IEEE Systems Journal, pp. 642-643, 2015.

[6] W. E. Dong, W. Nan, L. Xu, "QoS-Oriented Monitoring Model for Cloud Computing Resources Availability", In Proc. Int. Conf. on Computational and Information Sciences, pp. 1537-1540, 2013.

[7] X. Zheng, P. Martin, K. Brohman, L. D. Xu, "CLOUDQUAL: A Quality model for cloud services", IEEE Transactions on Industrial Informatics, Volume: 10, Number:2, pp. 1527-1536, 2014.

[8] S. Lee, D. Tang, T. Chen, W. C. Chu, "A QoS assurance middleware model for enterprise cloud computing", in Proc. IEEE Int. Conf. on Computer Software and Applications Workshops, pp. 322-327, 2012.

[9] G. Cicotti, L. Coppolino, R. Cristaldi, S. D'Antonio, L. Romano, "QoS monitoring in a cloud services environment: the SRT-15", Springer, pp. 15-24, 2012.

[10] M. J. DiMario, J. T. Boardman, B.J. Sauser, "System of Systems collaborative formation", IEEE Systems Journal, Volume: 3, Issue: 3, pp. 360-368, 2009.

[11] P. C. Hershey and Donald Runyon, "SOA monitoring for enterprise computing systems", In Proc. IEEE Int. Conf. on Enterprise Distributed Object Computing, pp. 443-444, 2007.

[12] P. C. Hershey and C. B. Silio, "Procedure for detection of and response to distributed denial of service cyber-attacks on complex enterprise systems", In Proc. IEEE Systems Conference (SysCon), pp.1-6, 2012.

[13] S. S. Chopade, K. U. Pandey, D. S. Bhade, "Securing cloud servers against flooding based DDoS Attacks", In Proc. IEEE Int. Conf. on Communication Systems and Network Technologies, pp. 524-528, 2013.