Providing Quality-Of-Service Observation and Response by System Of Systems In Cloud Computing Environments

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

Abstract

Cloud computing is a concept to offerglobal network access to a group of shared reconfigurable computing resources. Users and businesses may utilize cloud computing and storage solutions to store and process their data at other people's data centers in a variety of ways. Similar to a utility through a network, it depends on resource sharing to achieve coherence and economies of scale. The wider idea of shared services and convergent infrastructure is the basis of cloud computing. The quality of service (QoS) measures the entire performance of a computer or telephone network, especially as perceived by its users.The system provides a System of Systems approach in this project.Its purpose is to provide QoS administration, response, and monitoring for business systems which offer computing as service via cloud computing environment. A system of systems is made up of several task-focused or specialized systems which combine their resources and talents to produce a larger, more sophisticated system that provides greater capability and performance than the sum of its parts. It provides trustworthy QoS metric collecting and analysis implementation schemes, allowing cloud computing service providers &operations centers to satisfy pledged customer QoS requirements.

DOINumber: 10.48047/nq.2021.19.7.NQ21122 **NeuroQuantology2021;19(7):351-357**

1. INTRODUCTION

The quality of service (QoS) measures the entire performance of a computer or telephone network, especially as perceived by its users. Numerous connected factors of the network service, including as error rates, bandwidth, throughput, transmission latency, availability, jitter, etc., are frequently taken into account in order to quantify quality of service. Cloud computing is a concept that enables open access through a network to a common set of reconfigurable computing resources. It utilizes resource sharing, much like a utility (like the electrical grid through a network), to create uniformity and economies of scale. The efficacy of shared resources is another key goal of cloud computing, which includes dynamic resource reallocation in response to demand. This strategy enables several users to use a single server to receive and update their data without having to buy licenses for various applications, while also maximizing the use of computer resources, minimizing environmental impact, and minimizing costs.A system of systems is made up of many job-specific or specialized systems that combine their resources and talents to form a new, enhanced system. QoS refers to the capacity to assign distinct users, applications, or data flows differing priority or to ensure a specific level of efficiency for a data flow. By connecting systems into integrated system of systems, it is possible to achieve the interoperability and synergism of Computers,Control,Communications, Command, and Information (C4I) and Intelligence, Surveillance, and Reconnaissance (ISR) Systems. System of systems is large-scale parallel and decentralized systems, the components of which are also intricate systems. System of systems education includes the incorporation of systems into other systems which promote growth of social infrastructure. A strategy to

improve system development, integration, interoperability, and optimization for use in future combat scenarios is known as system of systems integration. Enterprise system of systems engineering are concentrated on fusing conventional operations in systems engineering with business processes like investment analysis and strategy development. The term "system of systems problems" refers to a class of cross-domain networks made up of disparate systems which display geographic spread, behaviorthat emerges, functional and administrative independence, and evolutionary growth. Systems engineering, complexity and design studies are all connected, but system of systems research also emphasizes the added difficulty of design.This article suggests a SoS method to offer QoS administration, response, and monitoring for corporate systems that provide computing as a service via cloud computing environment. The novel SoS technique is applied to a real-world problem using a specific example. In order to give business operators a simple and succinct perspective of QoS events inside cloud computing environments, this article presents a SoS. This enables rapid operator reaction to QoS issues. It also proactively notifies enterprise operators of the condition of the company. It gives ain-depth breakdown of the SoS technique and applies it to a cyber-security scenario where a distributed denial of service (DDoS) attack is launched against sophisticated cloud computing environment.

2. LITERATURE SURVEY

This study proposes a novel model that utilizes a grid of smart cards constructed in the context of SSL smart cards to address this problem. Researchers think that EAP-TLS serversmart cards provide the security and ease of use necessary for a dispersed server management. Researchers outline the design of a RADIUS server where SSL smart cards completely handle EAP messages. Finally, researchers discuss the specifics of the initial experimental findings using a 32-card Java card array and a RADIUS server to illustrate the viability and potential scalability of this design.This study proposes a novel modelthat utilizes a grid of smart cards constructed in the context of SSL smart cards to address this problem. Researchers think that EAP-TLS serversmart cards provide the security and ease of use necessary for a dispersed server management. Researchers outline the design of a RADIUS server where SSL smart cards completely handle EAP messages. Finally, researcher discuss the specifics of the initial experimental findings using a 32-card Java card array and a RADIUS server to illustrate the viability and potential scalability of this design.In this study, researchers suggest a design that divides the RADIUS server into two components. The RADIUS protocol is first processed by a pure software block. A smart card grid, which can accommodate 400 EAP-TLS smartcards, is the second option. It consists of a mother board and slave extensions, each of which can accommodate 32 smart cards. Manufacturers of mobile phones that want to verify their products' compatibility with SIM cards provided by several providers typically use this electronic rack. Each smart card is connected to a TCP socket, which serves as a virtual connection used to communicate with the RADIUS server. The EAP-TLS protocol is entirely handled by a tamper-resistant device [1].

However, as cloud computing becomes more widespread, consumers' demands for better, quicker, and more secure service delivery are stoked. As a result, authentication and access control have been researched as security challenges in cloud computing environment are always growing. Every time they utilize a novel cloud service in context of cloud computing, users must finish privateauthentication procedure mandated by the service provider. In the event that the characteristic and safety have been breached by any assault during this procedure, personal information that was held in database and business processing service is being revealed, or details pertaining to persons or companies will also be revealed. As a result, in the context of cloud computing, through provisioningthis study builds a framework for user authentication. A user typically registers by providing personal information, and after completing the registration process, the service provider gives the user with their own ID (identity) and an authentication method. Unfortunately, there is a chance that an attack during the authentication process might compromise the security and features of the authentication technique, which could lead to serious harm.Therefore, cloud computing user authentication has to be compatible and secure.The following aspects of the framework for user authentication that was proposed in this paper's context of cloud computing are included. The current cloud computing environment makes it difficult for customers to obtain user authentication since they must go through the procedure each time they use a service by utilising an ID and an authentication technique which service provider provides. So, the provisioning-based user authentication platform

eliminates current annoyance &makes it simple to access cloud computing services. Suggested platform architecture examines user data &verifies a client's identity using their user profile.Additionally, it has the benefit that while utilizing other Cloud Computing services, the user login procedure needed by the service provider may be skipped and user information is maintained through user monitoring [2].

Researchers introduce PasS (Privacy as a Service), a collection of security protocols used in cloud computing systems to guarantee the confidentiality and legal compliance of client data. By utilizing tamper-proof features of cryptographic coprocessors, PasS enables the safe processing and storage of users' private data. A safe execution area in the computing cloud that is both conceptually as well as physically secured from unwanted access is provided by the use of tamper-proof facilities. Additionally, PasS offers a privacy feedback mechanism that notifies client of the various privacy operations carried out on their data and alerts them to everypossible dangerswhich might endanger the safety of their sensitive data.We introduce PasS, a collection of security protocols used in cloud computing systems to guarantee the confidentiality and legal compliance of client data. A safe execution area in the computing cloud that is both conceptually as well as physically secured from unwanted access is provided by the use of tamper-proof facilities. Additionally, PasS offers a privacy feedback mechanism that notifies client of the various privacy operations carried out on their data and alerts them to everypossible dangerswhich might endanger the safety of their sensitive data.The privacy of client data in cloud computing infrastructures was ensured by PasS, a collection of security protocols, which were detailed in this work. To provide a safe and isolated implementation scenario in the cloud computing environment, security solution depends on securecryptographic coprocessors. The study discussed PasS protocols and provided a description of the privacy enforcement techniques they supported. The study also provided anexplanation of a privacy protocol proof of concept implementation. Future additions will: (1) consider various design options, including those that are independent of the existence of a trusted 3rdparty; (2) consider alternate key management and distribution mechanisms; (3) look into the creation of standard patterns to methodically support the software division process; &(4) provide in-depth examination &assessment of system implementation [3].

Regarding user trust and regulatory compliance, privacy is a crucial concern for cloud computing and must be taken into account at every stage of the design process. Key design concepts to handle these issues are provided in this study, which evaluates the privacy concerns that software developers confront while using the cloud as their production environment for offering services.Meeting the limitations on cross-border data transfer is a new problem, as is maintaining the standards of data protection and privacy needed by present regulations in cloud computing infrastructure. Cloud services bring privacy concerns and potentially reduce users' control since they process users' data on devices that the users do not own or run. Users' main worries with cloud computing adoption center on privacy issues, and unless technology solutions to ease users' fears are offered, this might be fatal for many different sorts of cloud services.Companies and governmental organizations are becoming more and more aware of the need for privacy-conscious design.The fact that organizations may share an off-premises infrastructure is one of the key features of cloud computing. Regarding user trust and regulatory compliance, privacy is a crucial concern for cloud computing and must be taken into account at every stage of the design process. Key design concepts to handle these issues are provided in this study, which evaluates the privacy concerns that software developers confront while using the cloud as their production environment for offering services.Meeting the limitations on cross-border data transfer is a new problem, as is maintaining the standards of data protection and privacy needed by present regulations in cloud computing infrastructure. Cloud services bring privacy concerns and potentially reduce users' control since they process users' data on devices that the users do not own or run. Users' main worries with cloud computing adoption center on privacy issues, and unless technology solutions to ease users' fears are offered, this might be fatal for many different sorts of cloud services.Companies and governmental organizations are becoming more and more aware of the need for privacy-conscious design.The fact that organizations may share an off-premises

infrastructure is one of the key features of cloud computing [4].

A strategy for providing accessible, on-demand network access to a shared pool of reconfigurable computer resources is known as cloud computing. On-demand self-service, ubiquitous network connectivity, location-independent resource pooling, quick flexibility, & measurable service make up its five key components. Depending on the underlying delivery and deployment patterns, applications running on or being created for cloud computing platforms present a variety of security and privacy problems. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the 3 main cloud delivery types. IaaS allows users to construct and operate applications on a set of virtualized infrastructure elements, such as storage and virtual machines (VMs), provided by the cloud provider. Programming environments may now access and use more application building elements thanks to PaaS, which clearly affects the application architecture.Clients purchase and utilize software components from various suppliers, while cloud providers enable and supply application software as on-demand services. Public, private, communal, and hybrid clouds are all types of clouds that may be deployed. The most promising method for resolving the semantic heterogeneity issue is an ontology, and an OWL-based framework is preferred to facilitate semantic heterogeneity management across various cloud providers. To guarantee that benefits of cloud computing are fully realized, existing security and privacy solutions must be critically reevaluated with regard to their suitability for clouds. Additionally, improvements to existing solutions as well as more mature and recent ones are urgently required. Since Cloud computing is just just getting started, how the security and privacy environment evolves will have an influence on how widely it is adopted [5].

3. PROPOSED SYSTEM

The proposed system provides a SoSmethod to offer QoS administration, monitoring, and reaction for business systems that provide computing as a service via cloud computing environment.This multidimensional paradigm offers an end-to-end viewpoint of system and allows for the positioning of metric perspectives both inside and outside of the conventional Open Systems Interconnection layers (infrastructure via applications/software) and SOA-based layers (business and governance).While SOA-based applications offer organizational& collaborative services which aid end users who are creating and consuming data utilizing software and infrastructure services, one authority delivers governance services across numerous heterogeneous administrative domains.Even though the constituent systems that make up a system of systems might differ greatly from one another and function independently, their interactions often reveal and offer significant emergent features. Stakeholders in these issues must be aware of, assess, and comprehend these emerging patterns' dynamic nature.

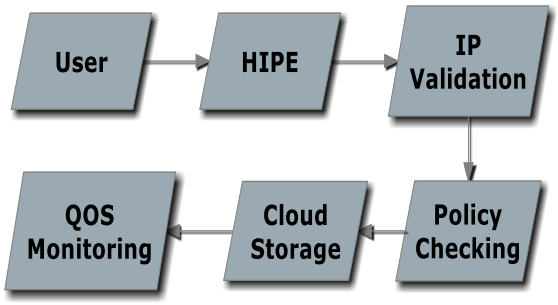

Fig 1 System Architecture

A new method of thinking about large-scale issues where interactions between technology, policy, and economics are the primary forces is supported by the system of systems approach. It makes no recommendations for particular devices, procedures, or techniques.Even while it is connected to the broad study of developing, complexities, and systems engineering, system of systems research additionally emphasizes the added difficulty of design. QoS refers to the capacity to assign distinct applications, users, or data flows differing priority or to ensure a particular level of efficiency for a data flow. In order to enable effective QoS administration, response, and monitoringthroughout various and different corporate operations centers, we define appropriate service-based QoS metric categories and metrics inside those categories.The metrics in the C&A metrics category serve to protect the security of systems, information, networks, applications, and databy identifying security risks and flaws, providing information to ensure that corrective action has been taken to address these flaws and weaknesses, and ensuring that remedial action has been implemented. Following section explains several stages that are involved in putting the suggested technique into practice:

Authentication:

To authenticate the identity of systems, users, or data sources. 1 or more techniques, including digital certificates, passwords, key exchange, and biometrics, may be used for authentication.

Confirming entity identity is a fundamental need for developing user trust in the service and making additional security features viable.

Authorization:

To report on resource access based on policy and authorization levels, both successfully and unsuccessfully. Authorization establishes an entity's rights (i.e., those tasks which may be entrusted to be carried out by the entity) beyond authentication, which just establishes an entity's identification. The least privilege concept is enforced through authorization metrics. The total service integrity is preserved and the efficacy of missions is increased by making sure that entities are given the lowest privileges possible while still fulfilling their objective.

Certification and Accreditation (C&A):

To determine degree to which a specific design and execution complies with a given list of security standards, a thorough assessment of technical and non-technical security elements of an IT system as well as other protections is undertaken in assistance with certification process.C&A security is required by the DoD Information Technology Security Certification and Accreditation Process. Metrics in the C&A metrics category help in detecting security risks and vulnerabilities, providing information to make sure that remedial measures are done to resolve these faults &weaknesses, &helping to ensure that systems, applications, networks,information, and data are safeguarded.

QoS Evaluation:

The amount of work finished over a certain period is described by throughput metrics. Metrics for throughput show how much work the application, team, machine, and network have completed. The right interpretation of these measures improves resource allocation, productivity, and efficiency. Delay Variation is the comparison of delays for various observation time periods. A few instances of delay variation involve the fluctuation in application response times among peak and off-peak hours, jitter, and from end to end delay variation in the order of packet arrival events. Delay variation detectssystem instability that either stops end users from effectively completing their tasks at the present time or that is a warning of issues that will do so in the future.

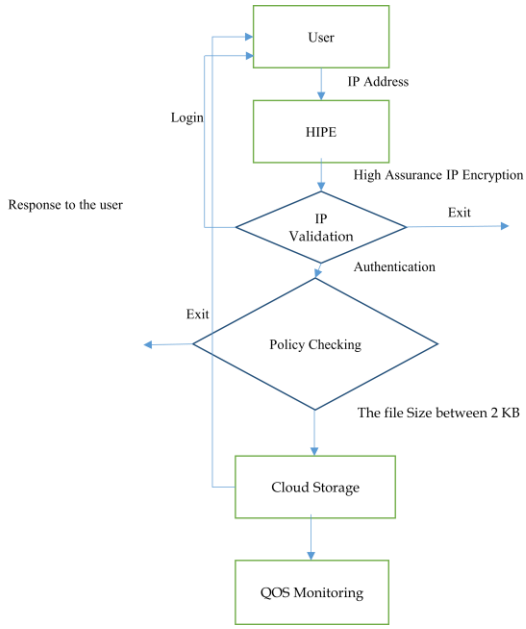

Fig 2: Flow Diagram

Performance Evaluation:

The system tracks three different times: 1) when a database query returns results (on the cloud instance hosting the database), 2) when application logic executes (on the cloud instance hosting the application server), and 3) when data is transferred over the network among application server and database server. When seen from the perspective of an application, throughput is determined by the quantity of transactions that have been completed, and is thus determined on the instance that houses the application server.

4. RESULTS

The term "cloud computing" refers to a concept that e nables public network access to a shared set of reconf igurable computing resources. A computer or telephone network's overall performance, particularly as seen by its users, is measured by the quality of service (QoS). This project offers a System of Systems technique to allow business systems that provide computing as a service via a cloud computing environment to respond, and monitor to QoS.System is made up of many task-specific or specialized systems that combine their resources and knowledge to produce a larger, more sophisticated system that provides greater features and efficiency than the sum of its parts. The throughput of the system is used as a barometer for overall performance, and the system's latency varies with time and depending on how the activity is carried out. This architecture is mature and has undergone extensive testing. A computer or telephone network's

overall performance, particularly as seen by its users, is measured by the QoS. To enable business systems that deliver computing as a service via a cloud computing environment to administrate, monitor, and react to QoS, this project offers a System of Systems methodology. The system is composed of numerous job-focused or specialized systems that pool their resources and expertise to develop a bigger, extra sophisticated system that provides greater features and efficiency than the sum of its parts.The throughput of the system is used as a barometer for overall performance, and the system's latency varies with time and depending on how the activity is carried out. This architecture is mature and has undergone extensive testing.

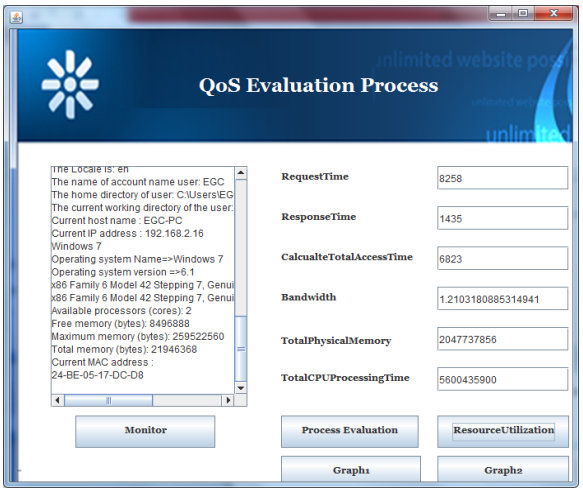

Fig 3: QoS Evaluation

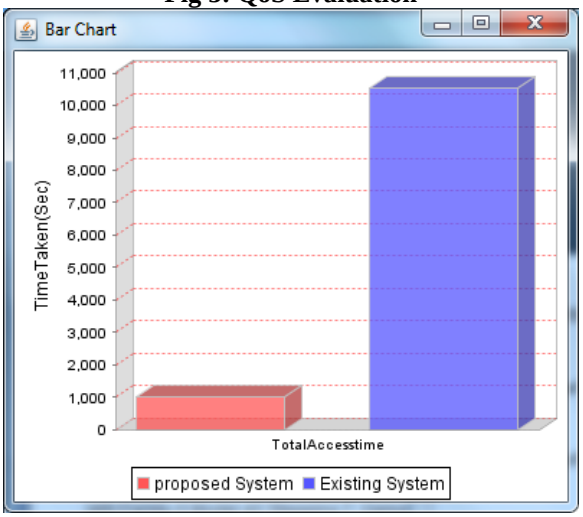

Fig 4: Performance Analysis (Time Taken)

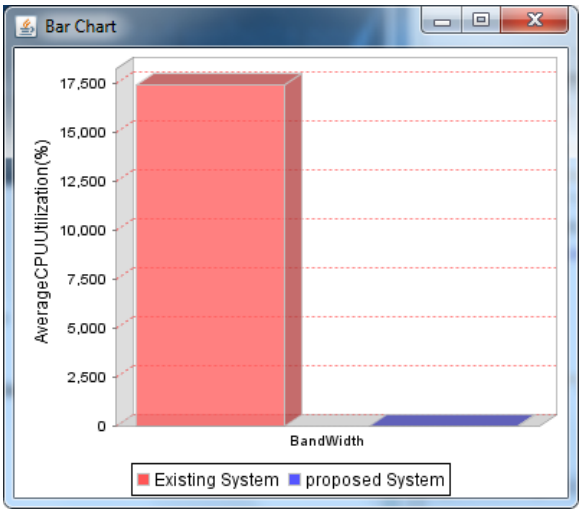

Fig 5: Performance Analysis (CPU Utilization)

5. CONCLUSION

The installation of trustworthy QoS metric collecting and analysis has been employed by the system in this project. With the help of a reliable QoS metric collecting and analysis implementation methodology, this method allows cloud computing service providers and operations centers to satisfy pledged customer QoS requirements. This plan expands on the conventional IaaS and SaaS monitoring, administration, and response to a full SOA stack that incorporates business logic (BaaS) and governance (GaaS).The first part of this application, which consists of two stages, is not dependent on database transactions, however the second phase requires three database transactions.The system's throughput serves as a gauge of overall performance. A high-throughput system in the cloud is wanted.A system of systems is made up of several job-focused systems that combine their resources and talents to produce a larger, extra sophisticated system that provides greater features and efficiency than the sum of its parts. It provides trustworthy QoS metric collecting and analysis implementation schemes, allowing cloud computing service providers and operations centers to satisfy pledged customer QoS requirements.The system assessed throughput at the application and database levels in this experiment. Even though delay is a crucial performance parameter, a system cannot be effectively characterised or monitored by only monitoring delay. The system's latency varies over time and when operations are carried out owing to a variety of reasons.The quality of service (QoS) measures the entire performance of a computer or telephone network, especially as perceived by its users.This architecture has been well-tested and is mature.

REFERENCES

[1] "An innovative solution for cloud computing authentication", P. Urien, E. Marie, and C. Kiennert, 2010.
[2] "User authentication platform using provisioning in cloud computing environment", H Ahn, H Chang, C Jang, E Choi, 2011.
[3] "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures", W. Itani, A. Kayssi, and A. Chehab, 2009.
[4] "Taking account of privacy when designing cloud computing services", S. Pearson, 2009.
[5] "Security and privacy challenges in cloud computing environments", H. Takabi, J. B. D. Joshi, and G. Ahn, 2010.
[6] "A Survey on QOS Guaranteed Bandwidth Shifting and Redistribution in Cloud Environment", Swati Nagpure, 2012.
[7] "Server-Side I/O Coordination for Parallel File Systems", Huaiming Song, Yanlong Yin, Xian-He Sun, Rajeev Thakur, Samuel Lang, 2011.
[8] "Parallel File System Analysis through Application I/O Tracing", S.A. Wright, S.D. Hammond, S.J. Pennycook, R.F. Bird1, J.A. Herdman, I. Miller, A. Vadgama, A. Bhalerao and S.A. Jarvis, 2013.
[9] "A Comparison Study between Informed and Predictive Prefetching Mechanisms for I/O Storage Systems", Maen M. Al Assaf, Ali Rodan1, Mohammad Qatawneh, Mohamed Riduan Abid, 2015.
[10] "QoS-Aware Bidding Strategies for VM Spot Instances: A Reinforcement Learning Approach Applied to Periodic Long Running Jobs", Marco Abundo, 2014.