Quality Measurement Model for Micro Level Ranking of IT and Bio Cloud Services

Saravanakumar K.[1] and Chitra S.[2]
1. Dept. of Computer Science & Engineering, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, INDIA
2. Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, INDIA

Abstract
Cloud Computing is an innovative, scalable and online outsourcing paying model by sharing of applications, platforms, networks, computational and storage services over internet called virtualized global paying technology. These resources can be dynamically reconfigured to meet the expectation of customers for optimum resource utilization called pay-per-use "Attachment Model" thru inter/intra networks. The service quality is the essential factor due to the increase of vast cloud services are pooled in the Digital Clouds market. Cloud service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Improving the quality of cloud services are the essential area of research. In this research work, we have developed an Improved Quality Measurement Model for Micro Level Ranking of Trusted Cloud Services called SPICER (Software Platform and Infrastructure Clouds Effective Ranker) with the necessary analysis and experiment results. Reviewed and studied the past and recent related works to support the quality improvement model of ranking cloud services. We have experimented for the development of integrated and micro level ranking of cloud services to support the ranking accuracy and complete coverage of business quality parameters on cloud flavours. That concept has applied to support, identify, categorize the widely used commercial IT and Bio-Tech related Apps for business consumers.

Keywords: Cloud flavours, SPICER Business trust advisor (SBeTA), CDDI registry, Dynamic profit optimizer, Integrated Dual Ranking (IDR), cloud service flavours.

Introduction

Cloud computing is the elastic behaviour of computing resources and services available to users to meet any needs. The core objective of the cloud computing is the resources are available as a service to any type of network users connected with the investment of less or zero capital. There is more number of cloud users benefiting thru the pay-per-use *"Attachment Model"*. The decision making is the one of the critical challenge of cloud users to identify the secure, optimum and trusted cloud service among the pool of cloud services increasing every day. So always there will be a need and demand of new method or protocol for selection of best quality of cloud services. The SPICER is a new approach to scan, analyse, evaluate the quality strength of various cloud services in terms of security, performance and cost economy factors before the cloud users' selection. The objective of ranking the cloud services is to actually helping users to observe, compare and take the decision among the different services [4]. Selecting the best service is impractical for cloud users to obtain the QoS information by evaluating them. Conducting real time service invocations is more tedious time and resource-consuming processes [31]. The long term observation of the QoS properties also a difficult to take quick decision in service selection. The cyber threats are the major challenges to all type of organizations to run their business via networks. Now days, the trust is shrinking rapidly from the internal and external staff who are involving the services to the cloud customers. Various types of cyber cheats are happening in very different and peculiar forms electronically. Many organizations also facing those problems and advising their customers to only follow the defined cloud policy rules to utilize the business clouds. There are various researches are going on for cloud computing environment and proposing the different models, implementation of their logics to tighten the level of security to enrich the performance. The increases of the cloud users to cloud providers are harmed by the recent security breaches. There is the one of the major reason that cloud users feels very critical, not comfortable to identify and selecting the services to meet their requirements, products and any physical computing resources safely.

Most of the research works specifically focused the any one particular type of the IT and Bio related cloud service models such as SaaS, PaaS and IaaS with the necessary parameters. Some of them have done their proposed trust model for selecting the cloud service by considering the limited QOS parameters. Their research related proposed models are very useful suggestions and recommendations to uplift the cloud users' confidents to trust the various cloud services.

In our research work, we reviewed and studied the most of the necessary customer requirements as various intensive parameters and proposed the most enhanced trusted model for cloud users as well as cloud service providers. Our trusted model will perform the three varieties of operations such scan, micro analyze and dual ranking of the cloud services. Supports to identify the business risks, security risks, mapping users requirements into QOS parameters, categorize the cloud services, dynamic research and prioritize to ensure the business and security trust among the various global cloud services thru the SPICER Business Trust Advisor (SBeTA). Initially this paper describing the critical and top security threats to cloud users and service providers. Secondly, it discusses about the existing cloud trust models and its concepts of ranking cloud services in the literature review. Thirdly our proposed model called SPICER architecture addresses the critical challenges by validating the QOS scanning, analysing and mapping, Micro level QOS value computation supports the rank accuracy, QOS attributes ranking prioritization, integrated dual ranking and cloud service profit optimization. The concept is applied to rank the common commercial and Bio business clouds.

The literature survey is really helpful to extract the static and real time QOS parameters to almost meet the users' expectations described in Section-II. In our model, the complete coverage given to the Security, performance and Cost economy related QOS properties. The section-III discusses about ranking prediction levels and final ranking sequences by dual ranking method. The Section-IV discusses about the comparative review of past and recent approaches. Finally the Section-V concluded with the future scope for the future enhancement.

Review of Literature

In [1] author proposed the trust model by computing the trust values based on the QOS parameters and discussed about the static and dynamic trust values. In [2], author explores about the ranking of cloud services by QOS attributes related to performance parameter. In [3] Author discussed about the ranking of cloud services and reservation with the limited QOS attributes. In [4] Author identified some 6 different approaches and their features have compared. In [5], Author reviewed the QOS parameters and discussed about the SaaS and IaaS cloud environment. In [6], Author identified the various characteristics of the popular service providers and reviewed their attributes .In [7], Author reviewed the security related issues of Cloud computing and proposed the method of computing the cost of security based on the multi level security model. In [8], author surveyed the popular existing models and concluded with the various securities related parameters.

In [9], Author presented about the the security and privacy challenges in cloud service models with the proposed security framework. In [10]. Author proposed a quality model to review and evaluate the service customizability of SaaS based on the attributes. In [11], Author reviewed the existing security models and mismatch of security services in the cloud service models based on the service dependency and highlights the need of technology improvement in security to face the cloud security attacks. In [12], Author reviewed the existing the cloud services trust mechanisms and highlights the need of improvement in security as well as the method has proposed for SLA between them. In [13], This paper describes about the security issues occurring in the PaaS delivery models and suggestions to cloud users and service providers regarding the implementation. In [14], This paper described about the comparative study of security provided at different cloud services in all the three service models using security parameters. In [15], Author described data related security challenges in the cloud environment with the and encryption methods to address the data security while transmitting the data via internet. In [16], this paper describes the ranking approach by service selection model with the limited QOS attributes. In [17], furnish the overall focus about the major issues in security and privacy specific to Infrastructure as a Service (IaaS) cloud service model. In [18], Author addressed various security attacks to the cloud environment using the real time case studies. In [19], Author describes about the security related threats and virtual partitions of data in the networks to strengthen the security level along with various encryption methods. In [20], Author explores the various risk factors of the cloud services and security risk management with the comparative review of security analysis models.

In [21], Author proposed a ranking model for selecting the service provider based upon cloud users requirements considering the billing cost and various parameters of cloud services. In [22], author presented the main challenges for security of IaaS and what are the solutions based on the security breaches. In [23], Author discussed about to apply the LP methods to cloud security and outsourcing capabilities. In [24], this paper presented to apply the linear programming conditions to support the enhancement of Cloud security. In [25], author identified the set of service primitives related to security issues on cloud storage with the performance analysis. In [26], The author reviewed the parameters affecting the cloud security and possible solutions for the security threats. In [27], Author described about the Cloud Computing security issues based on the surveys reports.

In [28], The Author, proposed the attribute based security mechanism with key generation for transactions. In [29], the Author has reviewed the performance and scalability of the existing file server systems in cloud environment and proposed the virtualization environment to eliminate the file storage and retrieval systems in file server. In [30], the author has reviewed the security challenges and presented the method of LP with possible secure computations on cloud environment.[31], This paper describes the QOS ranking of cloud services as a survey report. [32], [33] describes about the Cloud computing Apps for Bio-medical environment mostly used with computational biologists. The storage volume and complexity of bioinformatics data is increasing very faster with high-throughput bio-apps running machines are in more demand in the bio-cloud market.

Proposed Model-Spicer Architecture: After the detail review and study of related works, we have identified the major Challenges for the cloud service providers and cloud users who are running their business electronically using Cloud Computing thru Internet/Intranet. Then reviewed the massive cyber threats, business level challenges to the cloud owners, service providers and users. Then read and analyzed the possible suggestions with experiments provided as solutions to the business clouds for the trustful trades. There are enormous cloud services are increasing in the internet and to select the best quality and profit oriented cloud service is the major challenge to the cloud users. Conducting real time service invocations is more tedious time and resource-consuming processes for identifying the best service. There are many ranking approaches have proposed in the past 6 years with various experiments and result oriented solutions. That helps to uplift the propose of new models or protocols for ranking the cloud services is in more demand.

All the companies are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Most of the related works have concentrated the any particular category of the quality parameters such as security or performance or cost (pricing schemes) while ranking the cloud services. Few related works have proposed the common approaches to cloud flavours. In our work, we have reviewed those related works and their stated concepts supporting to design our proposed model. We have almost gathered the QOS properties for micro level ranking computation to ensure the trust and accuracy of ranking the business clouds. Categorized and distributed under the 3 important quality parameters as security, performance and cost economy parameters addressing the quality and accurate measurements while ranking the cloud services. Concentrated the related text books and articles for the further improvement of our proposed model enforcing the necessary formulas for regulate and shape the accuracy of rank analysis, cloud service strength analysis, review of security, performance, cost factors and integrated dual ranking by prioritization. This model focusing the major business objectives of cloud service providers and Cloud users.

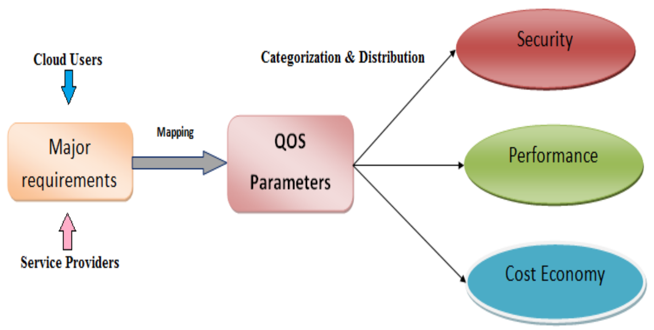


Figure 1: QOS Mapping process

- Security parameters → Computes security risks and trust values
- Cost parameters → Computes the business risks and trust values
- Performance parameters → Computes the utility, user expectation risks and trust values

In our model, all the requirements have mapped and distributed to security, performance and cost economy quality parameters. The sub parameters also derived from them. Numeric weitages have assigned with the scale of rating to organize in the sequence order of ascending to various cloud services. This will help and support the micro level analysis to trace the unique strength of QOS attributes. Then based on the review, the QOS parameters have identified for security, performance and cost economy factors. This is achieved by enforcing the ranking prioritization rules discussed in the section-III.

The following table describes the comparative review of various articles recently published in the internet about the critical and massive security threats After the overall review, all the necessary parameters related to security have identified based on the careful study of following articles and most common parameters have marked in the comparative review tabulated here.

Coverage of QOS Suite:

- The parameters for the SaaS
  - Key Security Parameters
    - ✓ Identity management, Data Protection, Assurance, Security Certifications, Disaster recovery polices, protective technologies (Encrypted storage), Security monitoring (Cyber Threats), Independent security audits, Testing of Version tracking, Pen Test and periodical updates of Security Codes.
  - Key Performance Parameters
    - ✓ Average response time, interoperability, Internet Downtime Rate, Frequency of Failure, periodical updates of Application Service Drivers(ASD), Frequency of Successive operations, Increase/ Decrease rate of throughput, Availability, Usability & Scalability
  - Key Cost Parameters
    - ✓ Pricing Policies, Storage Allocation/ Month, Pricing per user/Month, Free trail facility, license cost, implementation cost, administrator cost, long time user benefits, additional charges, Agility option
- The parameters for the PaaS
  - Key Security Parameters
    - ✓ Network Security
      - Encryption, Intrusion detection, traffic clean
    - ✓ Service Security
      - Authentication, authorization, vulnerabilities scanning, data isolation and virus detection.
    - ✓ Storage Security
      - Encrypted storage, Access control, data protection, integrity
  - Key Performance Parameters
    - ✓ Interoperability, flexibility, Average Response time, computation time, communication time, CPU load

(%), Accuracy, Reliability, Packet loss frequency, Multilanguage support

○ Key Cost Parameters

✓ Capital cost, development cost, deployment cost, maintenance cost, testing cost, application storage period cost, application users utilization cost, Agility option

➢ The parameters for the IaaS

○ Key Security Parameters

✓ Trust worthy certifications, third party audit compliance, Automated monitoring tool, Data protection, Intrusion detection and prevention, disaster recovery policies, Security focus on Operating Systems, firewall with future updates, Physical security provisions, external interface protection

○ Key Performance Parameters

✓ Interoperability, Average Response time, computation time, communication time, CPU load (%), Accuracy, Packet loss frequency, Automated monitoring tool

○ Key Cost Parameters

✓ Cost of 'Instance Hours', CPU utilization cost, Network & IO read/write Cost, Data transfer (in/Out) cost, Firewall cost, storage period cost, DB Transactions cost, IP cost, Additional cost

Table 1
Comparative review of articles related to security threats

S.N.	Article-I Top 12 cloud computing threats in 2016-March www.infoworld,com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html	Article-II Top 10 Security Concerns for Cloud-Based Services security (https://www.incapsula.com /blog/category/security) · December 14, 2015	Article-III The top 10 cloud computing threats and vulnerabilities www.coalfire .com/top10 risks-in-the-cloud.pdf	Article-IV 9 Worst Cloud Security Threats www.informationweek.com/cloud/iaas/9-worst-cloud-security-threats/d/d-id/1114085?page_number=2	Article-V www.altiusit.com /files/blog/Top10 Cloud Computing Threats.htm
1	Data breaches	Data breaches	Reduced Governance	Data breaches	Changes in business model
2	Permanent Data loss	Data loss	Data location	Data Loss	Data loss & Leakage
3	Weak identity, credential and access management	Hijacking of Accounts	Data ownership	Account Or Service Traffic Hijacking	Accounts Hijacking
4	Insecure APIs	Insider Threats	Increased attack surface	Insecure APIs	Insecure interfaces
5	System and application vulnerabilities	Malware Injection	New attack vectors	Abuse of Cloud Services	Insecure Cryptography
6	Account hijacking	Abuse of Cloud Services	Low visibility into virtual networks	Malicious Insiders	Abuse
7	Malicious insiders	Insecure APIs	Identity federation	Insecure APIs	Malicious insiders
8	Advanced Persistent Threats (APTs)	Denial of Service Attacks	Reduced monitoring	Denial of Service	Risk profile
9	Insufficient due diligence	Shared Vulnerabilities	Extreme outages	-	Users
10	Abuse and nefarious use of cloud services	Poor recovery procedures	Value concentration	-	Hackers and evesdroppers
11	Denial of Service	-	-	-	Cloud API Vulnerabilities
12	Shared technology issues	-	-	Shared technology	Shared technology

The following formulas compute the QOS property values of parameters with the numeric weightages computed within the 10 point scale measurement for ranking.

$$TSSaaS = \sum_{i=1}^{s1} WS_{Si} + \sum_{j=1}^{p1} WS_{Pj} + \sum_{k=1}^{c1} WS_{CEk} \quad (1)$$

$$TSPaaS = \sum_{l=1}^{s2} WP_{Sl} + \sum_{m=1}^{p2} WP_{Pm} + \sum_{n=1}^{c2} WP_{CEn} \quad (2)$$

$$TSIaaS = \sum_{p=1}^{s3} WI_{Sp} + \sum_{q=1}^{p3} WI_{Pq} + \sum_{r=1}^{c3} WI_{CEr} \quad (3)$$

$RnkPrdS_1(C_i) = Rnk[r_j]$ where i = 0 to N; j= 1 to 10;

The WS_{Si}, WS_{Pj} and WS_{CEk} are trust value parameter with the S_i, P_j and CE_k are QOS parameters as follows the other main and sub parameters. There are 11 different cloud vendors have considered for same type of cloud service in SaaS model.

There are thousands of IT and Biological related cloud services are available at free or low cost. But obtaining the real data from vendors is impossible for surveying. The data provided are collected from the few companies with the legal authorization and applied in our model. The Quality parameters have stored in matrix form with the observed values lies between 0 to 1 for ranking computation of Security, performance and cost economy category.

QOS matrix for Cloud Service$_i$ on the SaaS flavour.

S_rS_{aaS}= C[i]Q[j]={Q[i][j] .....Q[n1][n2]};
S_rP_{aaS}= C[i]Q[j]={Q[i][j] .....Q[n3][n4]};
S_rI_{aaS}= C[i]Q[j]={Q[i][j] .....Q[n5][n6]};

The trust value of each parameter should be 0 to 1 as per the defined category.

{0-0.25 → Poor; 0.26-0.50 → Average; 0.51-0.75 → Above average; 0.76-1.0 → Good}

The Trust values will be computed, ranked and compared in three prediction rounds.

Prediction round-I: Trust value computation of static QOS properties.

Prediction round-II: Trust value computation of Security, performance and cost economy parameters.

Prediction round-III: Trust value computation of dynamic QOS properties.

Then finally the Micro level ranking algorithm will scan and analyse the past prediction rounds and generate the final rank list.

Table 2
QOS Security Trust Score Matrix

CSi\QOSj	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	$SC_iA_{vg}TV$
C1	1	0.75	0.25	0.5	0.5	0.75	0.25	0	0.5	0	0.5	4.55
C2	1	0.5	0.25	0.5	0.5	0.5	0.5	0.25	0.25	0	0.5	4.32
C3	0.5	0.75	0.5	0.75	0.75	0.5	0.5	0.5	0.75	0.5	0.5	5.91
C4	0.75	0.5	0.5	0.75	0.5	0.5	0.5	0	0.5	0	0.5	4.55
C5	1	0.75	0.75	1	0.75	0.75	0.75	0.5	0.75	0.75	0.75	7.73
C6	1	0.5	0.75	0.75	0.5	0.75	0.75	0.5	0.5	0	0.5	5.91
C7	1	0.75	0.5	0.5	0.5	0.5	0.75	0.5	1	0.5	0.75	6.59
C8	1	0.75	0.5	0.5	0.5	0.75	0.75	0.5	0.5	0.5	0.5	6.14
C9	1	0.5	0.75	0.5	0.5	0.75	0.5	0.5	0.5	0.5	0.5	5.91
C10	0.75	0.5	0.5	0.75	0.75	0.5	0.5	0.5	0	0	0.75	5.00
C11	1	0.75	0.75	0.75	0.5	0.75	0.5	0.5	0	0	0.5	5.45

Table 3
QOS Performance Trust Score Matrix

CSi\QOSj	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	$SC_iA_{vg}TV$
C1	0.75	0.5	0.25	0.25	0.75	0.75	0.75	0.75	0.75	0.5	5.25
C2	0.5	0.5	0.5	0.5	0.5	0.5	1	0.5	0.5	0.5	5
C3	0.75	0.25	0.25	0.5	0.5	0.5	1	0.5	0.5	0.75	4.75
C4	0.5	0.5	0.5	0.5	0.5	0.5	0.25	0.5	0.5	0.75	4.5
C5	0.5	1	0.5	0.25	0.75	0.75	0.5	0.5	0.75	0.25	5.25
C6	0.75	0.5	0.75	0.25	0.75	0.5	0.5	0.5	0.75	0.5	5
C7	1	0.75	0.75	0.25	0.75	0.75	0.75	0.75	0.75	0.75	6.25
C8	0.5	0.5	0.5	0.25	0.75	0.5	0.5	0.5	0.5	0.5	4.5
C9	0.75	0.5	0.5	0.25	0.75	0.5	0.5	0.75	0.5	0.5	4.75
C10	0.5	0.5	0.5	0.25	0.75	0.5	0.75	0.5	0.5	0.5	4.75
C11	0.75	0.25	0.25	0.5	0.5	0.5	0.75	0.5	0.5	0.75	4.5

Table 4
QOS Cost Economy Trust Score Matrix

CSi\QOSj	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	$SC_iA_{vg}TV$
C1	0.75	1	1	1	1	1	1	0	1	0	7.75
C2	0.5	0	0	1	0	1	1	0	1	0	4.5
C3	0.75	1	1	1	0	1	1	1	0	0	6.75
C4	0.75	1	1	0	1	0	1	1	1	0	6.75
C5	0.5	0	0	0	1	1	1	0	1	0	4.5
C6	0.25	1	1	1	1	1	1	1	1	0	8.25
C7	0.75	1	1	1	1	1	1	1	0	1	8.75
C8	0.75	1	1	1	1	0	1	1	1	0	7.75
C9	0.5	1	1	1	1	0	1	0	1	0	6.5
C10	0.5	0	0	0	1	1	1	1	1	1	6.5
C11	0.75	1	1	0	1	1	1	1	1	0	7.75

Table 5
QOS Prediction Round-I Trust Rank Matrix

CSi\QOSj	Wssi	Wspj	Wscek	WciSaaS
C7	6.59	6.25	8.75	7.20
C6	5.91	5	8.25	6.39
C8	6.14	4.5	7.75	6.13
C11	5.45	4.5	7.75	5.90
C1	4.55	5.25	7.75	5.85
C5	7.73	5.25	4.5	5.83
C3	5.91	4.75	6.75	5.80
C9	5.91	4.75	6.5	5.72
C10	5	4.75	6.5	5.42
C4	4.55	4.5	6.75	5.27
C2	4.32	5	4.5	4.61

Computation of Dynamic QOS Suite:

(D1) Service Response Time of Cloud Service$_i$:

$\sum_i T_i/n$ ➔ (r1+r2+r3+r4+r5)/5= (19/5) = 3.8 Seconds
Average Response Time is given by $\sum_i \mathbf{T_i/n}$ where is time between when the user i requested for a service and when it is actually available and n is the total number of service requests

(D2) Suitability: Number of non-essential features provided by service/Number of non-essential features required by the customer
$NCSP_{NEFi}/ nCUR_{NSFj}$ ➔4/2= 2 *100 = 200%

(D3) Accuracy: The accuracy of the service functionality measures the degree of closeness to user expected actual value or result generated by using the service. If f_i is the number of times the Cloud provider fails to satisfy promised values for user i over the service time T, then accuracy frequency is defined as $\sum_i f_i/n$ where n is the number of previous users.
n=7; $f_{i=\{1,0,0,0,1,0,0\}}$ ➔ 2/7 = 0.286*100=28.57%; 5/7*100 is the % of Accuracy➔71.42%

(D4) Interoperability: Interoperability is the ability of a service to interact with other services offered either by the same provider or other providers. It is more qualitative and can be defined by user experience.

Number of platforms offered by the provider/ Number of platforms required by users for interoperability

(D5) Availability: The objective of the availability is to ensure that availability of the services delivered to the customer meets or exceeds the committed needs of the customer. Availability is determined by reliability, maintainability, serviceability, performance and security. The following available calculation is often based on the agreed service time and downtime.
Availability=[(Agreed Service Time – Downtime)/ Agreed Service Time]*100
The availability will be calculated for the every cloud service/product in the form of %.

(D6) Usability: The ease of using a Cloud service is defined by the attributes of Usability. The components such as operability, learnability, installability and understandability can be quantified as the average time experienced by the previous users of the Cloud service.

(D7) Credibility of Services

This is the important factor influencing the long term performance of the Cloud Services. The trustworthiness of the internal and external staff will be given as feedback by cloud users experiences.

SPICER Prediction Rounds for Integrated Ranking Process

The QOS attributes will be classified and ordered in the three categories as security, performance and cost for all the three service models. According to that and prediction round-I, total strength of the each cloud service$_i$ will be evaluated and ordered in the ascending sequence. The trust score matrix will be formed based on the individual strength of the QOS attributes and the total trust rank matrix will be formed. Then ranking prioritization will be applied to the score arrays to analyze and filter the cloud services having top score in security, performance and cost economy attributes. The ranking algorithm will continue to perform the micro level ranking of computation in prediction round-III with the dynamic attributes such as $\{D_1, D_2, D_3....D_n)$. The attributes are real time attributes to observe the functional behaviour of the each cloud service. The numerical computation will be performed with the standard formulas. Then the dynamic trust rank matrix will be computed with the user experiences distributed as formulas. Then ranking scores generated in the prediction round-II will be sent to Dynamic iCloud Micro Survey Ranker to compute the final rank list of cloud services. It is called dual ranking or integrated ranking.

QOS Ranking as per Trust value computation based on the total score in prediction -I (Static)

R1 R2 R3 R4 R5➔ {C7, C6, C8, C11, C1}

Prediction Round-II of QOS Ranking

➔{C5, C7, C8, C3, C6} ϵ WS_{Si}
➔{C7, C1, C5, C2, C6} ϵ WS_{Pi}
➔{C7, C6, C1, C8, C11} ϵ WS_{CEi}
➔{Here the Ranking prioritization will be formed to prefer high weightages to the cloud services who are having highest total trust value in security and performance and then Cost economy parameters}

Strength Level	Security	Performance	Cost EC
9-10	1.0	0.80	0.70
8-9	0.80	0.75	0.65
7-8	0.70	0.65	0.50

R1 R2 R3 R4 R5➔ {C7, C5, C6, C8, C1}

Comparing and analysing the accuracy of Prediction round-I with Round-II forms the following rank sequence.
R1 R2 R3 R4 R5
QOS Dynamic Ranking as per Prediction-III:
R1 R2 R3 R4 R5 R6 R7 R8
➔{C7, C5, C6, C8, C1, C11, C9, C3}

The purpose of micro level computation is to maintain the state of each QOS attribute in static and dynamic QOS repository arrays to locate and calculate the strength of the particular cloud service. The SPICER ranking algorithm will do the final computation to reconfirm the quality of ranking accuracy.

Analysing and Comparing the Prediction Round-II with QOS Ranking as per total score-II (Dynamic)

➔ {C7, C8, C6, C5, C1, C11, C9, C3}

After the micro level prediction analysis and integrated comparison, the best cloud services filtered to close to the final ranking accuracy in prediction round-III. The final Selection of the Cloud services with the ranking order has computed based on the comparison and filtering of pre-determined weightages. Comparing and analysing the accuracy of Prediction round-II with Round-III forms the following rank sequence

R1 R2 R3 R4 R5 R6 R7
➔ **{C7, C5, C6, C8, C1, C11, C3}**

➔{C7, C5, C6, C8, C1}

The data calculated are samples observed from the various users' survey reports. Users experiences observed as realtime experience metrics.

Table 6
QOS Prediction Round-III Trust Rank Matrix

CSi\QOSDj	D1	D2	D3	D4	D5	D6	D7	Quality Strength
C7	7	7.5	9	7.5	7	9.8	8	7.97
C8	7	7.7	9.3	8	6	9.62	8	7.95
C6	8	6.5	8	7	7	9.7	8	7.74
C5	7	7.4	9	7	6	9.27	7.5	7.6
C1	7	7.3	7.45	6	7	9.37	9	7.59
C11	7	7	7.21	7	7	9.72	8	7.56
C9	6.5	6.2	8.67	7	7	9.65	7	7.43
C3	6	6	7.8	6	6	9.7	8	7.07
C4	6	5.9	8.42	5.5	6	8.92	7.5	6.89
C10	6.3	5.7	7.9	5	6	8.58	7.5	6.71
C2	5.4	5.5	8	5.8	5	8.73	7.5	6.56

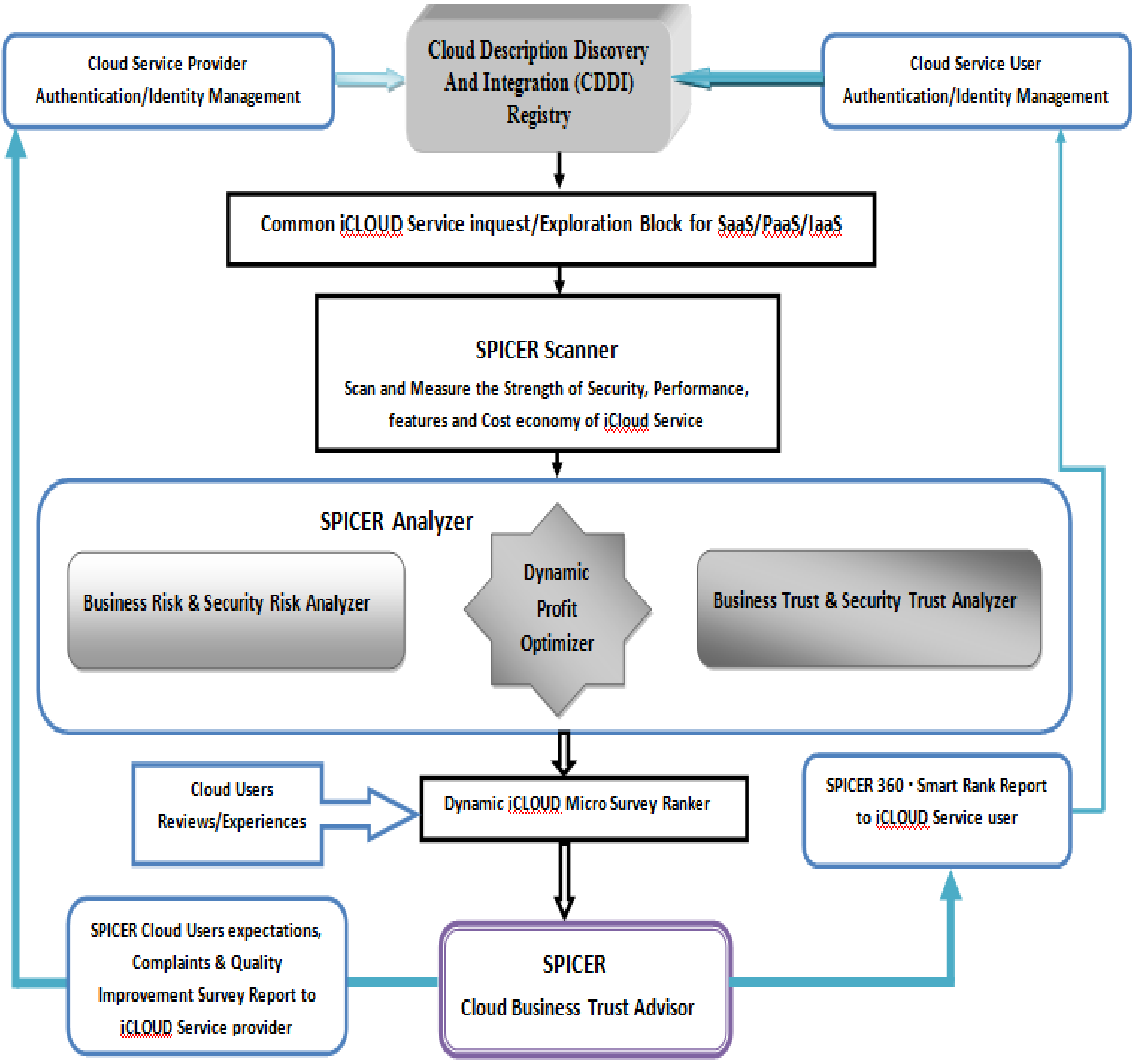


Figure 2: Architecture of Software Platform and Infrastructure Efficient Ranker (SPICER)

Description of SPICER modules

- Registering the Cloud Service type in a Tera space cloud storage repository called Cloud Description Discovery & Integration Registry (CDDI). Cloud users and service providers can request and identify the history of registered cloud services and their ranking profiles after their proper identity registration and confirmation.
- Service inquest/exploration Block is used to scan, analyze and indentify the type of cloud service using the iCLOUD inquest algorithm. Categorize and store the cloud services in to the SaaS, PaaS and IaaS arrays called Service Flavor data storages.
- SPICER-Scanner: Scan the Key Quality Indicators (KQI) with the numerical values
for that security, performance and cost economy parameters of iClouds and calculate the strength.
- Set the numeric quality weightages to the sub parameters of security, performance and cost main parameters to map in to QOS attributes for static and dynamic ranking.
- The storage volume and complexity of bioinformatics data is increasing very faster with high-throughput bio-apps running machines are in more demand in the bio-cloud market. As a result, many of the biotech companies, research institutes, pharmaceutical companies, and computational labs requires cloud computing as a cost-effective alternative to process and store this vast amount of biological data[32]. So this model exclusively proposed for various IT and Bio-informatics related business clouds.
- Quantify the main parameters with the summated QOS attribute values using the arithmetic progression method for security, performance and cost sub parameters of each cloud services in the scanner module.
- SPICER-Analyzer: It is a core module of the SPICER having the ranking research primitives. Business Trust & Security Trust Analyzer will scan and analyze the strength of the business and security parameters.
- The trust values will be analyzed in Business Risk & Security Risk Analyzer to calculate the risk factors of each cloud services. SPICER analyzer will do the final calculation by scanning and investigating the static ranking weightages. The security parameters mapping in to security risks, cost parameters mapping in to business risks and performance parameters mapping in to utility and user expectation risks. This component analyzing the each cloud service having good strength in security and performance parameters will be preferred when compared with cost economical scenario.
- Generate the final decisions based on the previous three ranking prediction rounds for final decision. The final decision will be reviewed with the previous stages of ranking predictions, ranking prioritization, strength value of security, performance and cost economy factors comparison applying the static and dynamic quality parameters. Then generating the final ranking order of cloud services by integrated/dual ranking. Then it prepares and sends the two different survey reports to cloud users and service providers based on the requests. smart rank report with the complete coverage of ranking survey parameters to meet the user expectations and Quality Improvement Survey report to service providers for fact finding, sustaining and knowing the current and future requirements of the users/customers.
- This method of ranking is increasing the accuracy with the concern of strength of essential parameters as security, performance and cost applicable to SaaS, PaaS and IaaS oriented cloud vendors. The SaaS vendors may be customers to PaaS by storing their application in the platform. The PaaS providers may be customer to IaaS vendors where their platform environment is running in the physical infrastructure. So the SPICER CDDI registry can store, retrieve ranking of various types of cloud services.
- Dynamic iCloud Survey Ranker(iCSR) is used to collect, order and categorize the past user experiences of the registered cloud services already registered in the CDDI registry. The user feedbacks will be normalized to standard parameters form with numeric weightages for calculating and generating dynamic ranking. Then applying and performing the past user experiences in essential parameters in ranking prediction round$_i$. Then the ranking order of cloud services will be stored in matrix form will be sent to Cloud Business Trust Advisor (CBeTA).
- Cloud Business Trust Advisor (CBeTA) plays the vital role to compare, analyze all the three prediction rounds and generate the final decisions. It will be reviewed with the previous stages of ranking predictions, ranking prioritization and strength value of security, performance and cost economy factors comparison applying the trust score of static and dynamic QOS parameters. Then generating the trust reports for the users and service providers. It prepares and sends the two different survey reports to cloud users and service providers based on the requests. smart rank report with the complete coverage of ranking survey with the user expectations and Quality Improvement Survey report to service providers for fact finding, sustaining and knowing the current and future requirements of the users/customers.
- This method of ranking is increasing the accuracy with the concern of strength of essential parameters as security, performance and cost applicable to SaaS, PaaS and IaaS oriented cloud vendors. The SaaS vendors may be customers to PaaS by storing their application in the platform. The PaaS providers may be customer to IaaS vendors where their platform environment is running in the physical infrastructure. So the SPICER CDDI registry can store, retrieve ranking of various models of cloud services.

Comparative review of past and recent approaches: There are six different ranking approaches have studied and reviewed with their approaches. The QOS based ranking approaches in the related works are having concept similarity with limited QOS attributes. Some of the approaches are using the mathematical formulas and ranking then cloud services only based on the highest scores. Few related works extended the above with identifying the past cloud users feedbacks with their positive and negative opinions (identical and non-identical experiences). This is essential for the mapping in to the dynamic ranking attributes to ensure and improve the quality of ranking. But the coverage of QOS parameters and accuracy of the measurements in those proposed models need to be broadening in their approaches. Most of the ranking approaches are specifically focusing the any one service model or considering the general/limited QOS attributes in their ranking algorithms may not be sufficient to determine the accurate of ranking. Based on the various reviews, online articles related to ranking, cloud security, performance and cost economical factors, our research work has proposed as model to meet the customers' business objectives in SaaS, PaaS and IaaS service models. The accuracy of ranking is important to identify the high quality of cloud applications and resources to be utilized by users without spending cost, time and multiple service invocations. The various ranking approaches have reviewed and tabulated based on their attributes and behaviours.

How the proposed system enhanced?

✓ The coverage of the QOS attributes are categorized and distributed in terms of security, performance and cost economy factors for supporting IT and Biological Cloud Apps.

✓ This model serving the micro level ranking of the cloud services by analyzing and calculating the strength of each QOS to improve the accuracy of ranking of cloud services.

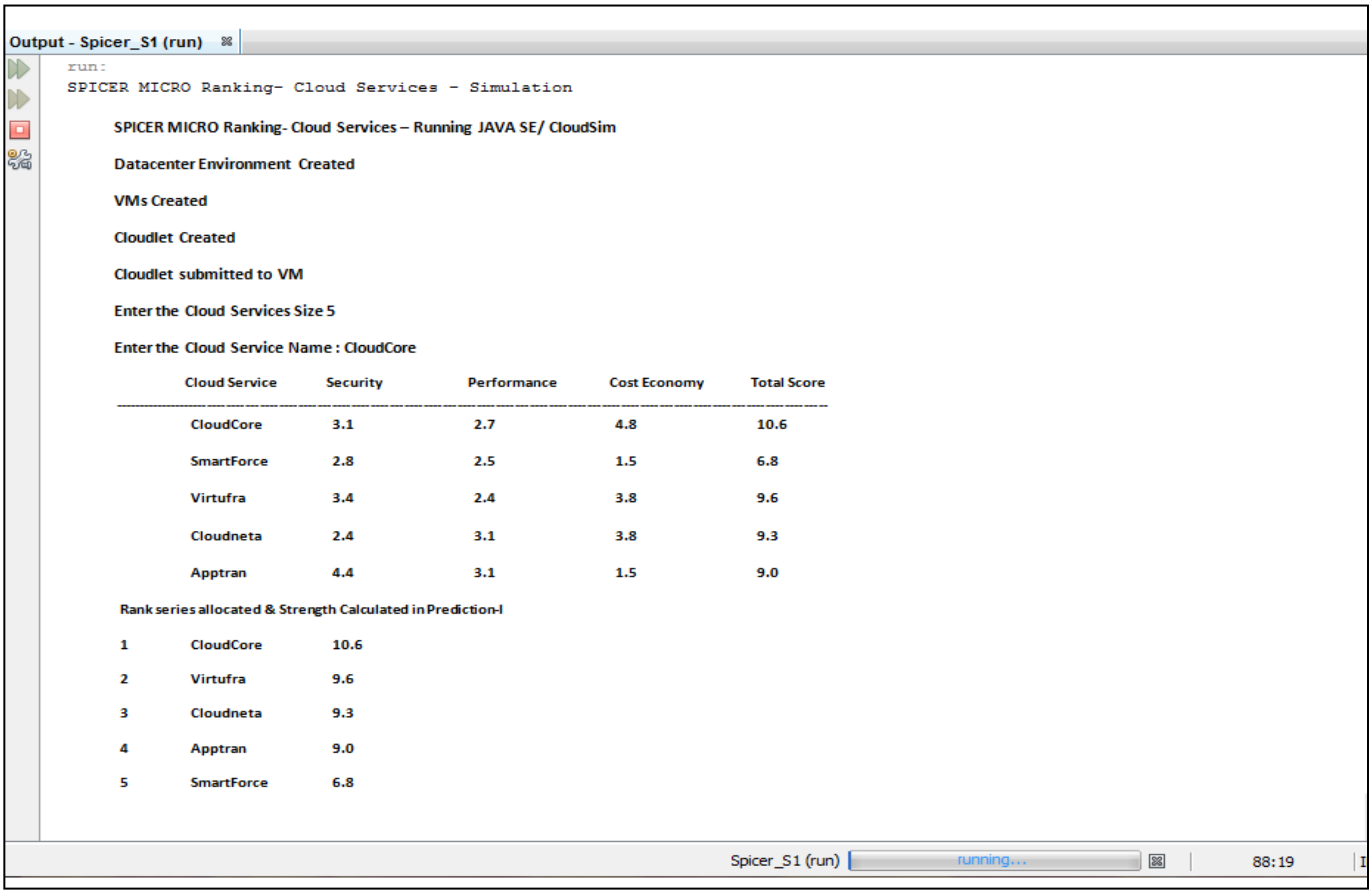
✓ The security is the most important parameter because the most of the customers prefer the security and performance rather than the cost. The particular service is very lower cost but poor security may lose the business as well as customers business goals. Our algorithm has proposed according to that most trust points of business customers by incorporating the SPICER ranking prioritization algorithm.

✓ Supports the cloud users while selecting the Cloud Services/Vendors by tracing the missing QOS parameters in the past approaches. It helps to Cloud Users to select their desired services to meet their requirements traceable to customer budget.

Supports the unique retrieval of any QOS attributes to analysis in different dimensions. It is a Good service monitor and spectator.

The following reports show the results and findings of Cloud services using SPICER ranking algorithm.

The following table shows the comparative review of SPICER model with the ranking approaches.


Output - Spicer_S1 (run)
run:
SPICER MICRO Ranking- Cloud Services - Simulation
SPICER MICRO Ranking- Cloud Services – Running JAVA SE/ CloudSim
Datacenter Environment Created
VMs Created
Cloudlet Created
Cloudlet submitted to VM
Enter the Cloud Services Size 5
Enter the Cloud Service Name : CloudCore

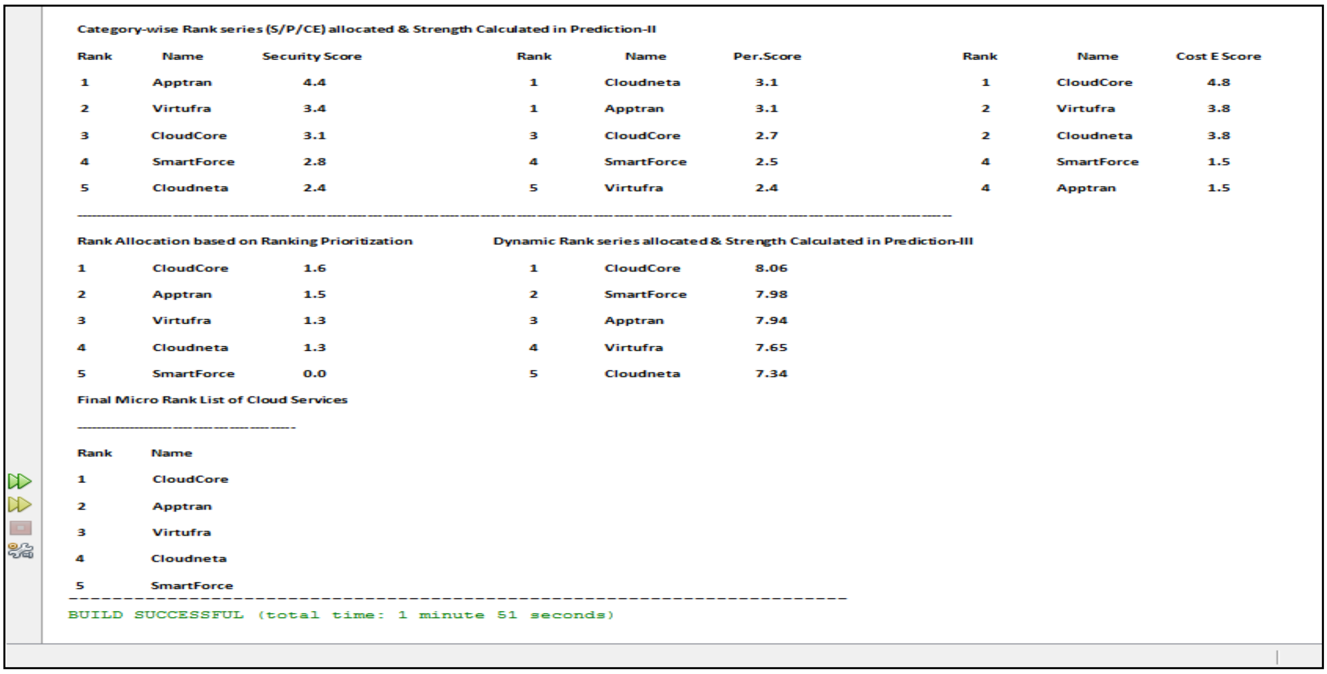
Cloud Service	Security	Performance	Cost Economy	Total Score
CloudCore	3.1	2.7	4.8	10.6
SmartForce	2.8	2.5	1.5	6.8
Virtufra	3.4	2.4	3.8	9.6
Cloudneta	2.4	3.1	3.8	9.3
Apptran	4.4	3.1	1.5	9.0

Rank series allocated & Strength Calculated in Prediction-I

1	CloudCore	10.6
2	Virtufra	9.6
3	Cloudneta	9.3
4	Apptran	9.0
5	SmartForce	6.8

Spicer_S1 (run) running... 88:19

Figure 3: Result verification of rank prediction round-I



```
Category-wise Rank series (S/P/CE) allocated & Strength Calculated in Prediction-II
Rank    Name         Security Score        Rank    Name         Per.Score        Rank    Name         Cost E Score
1       Apptran      4.4                   1       Cloudneta    3.1              1       CloudCore    4.8
2       Virtufra     3.4                   1       Apptran      3.1              2       Virtufra     3.8
3       CloudCore    3.1                   3       CloudCore    2.7              2       Cloudneta    3.8
4       SmartForce   2.8                   4       SmartForce   2.5              4       SmartForce   1.5
5       Cloudneta    2.4                   5       Virtufra     2.4              4       Apptran      1.5
------------------------------------------------------------------------------------------------
Rank Allocation based on Ranking Prioritization        Dynamic Rank series allocated & Strength Calculated in Prediction-III
1       CloudCore    1.6                   1       CloudCore    8.06
2       Apptran      1.5                   2       SmartForce   7.98
3       Virtufra     1.3                   3       Apptran      7.94
4       Cloudneta    1.3                   4       Virtufra     7.65
5       SmartForce   0.0                   5       Cloudneta    7.34
Final Micro Rank List of Cloud Services
------------------------------------
Rank    Name
1       CloudCore
2       Apptran
3       Virtufra
4       Cloudneta
5       SmartForce
------------------------------------------------------------------------------
BUILD SUCCESSFUL (total time: 1 minute 51 seconds)
```

Figure 4: Result verification of rank prediction round-II & III

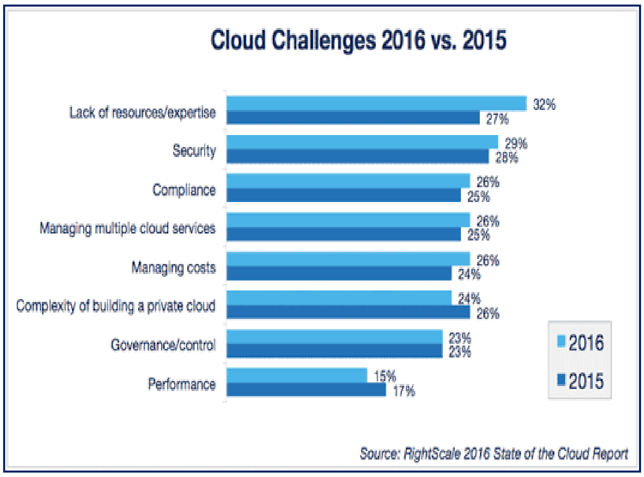
Table 12
Comparative report of Ranking Approaches

Proposed Scheme	Period	Consideration of QOS attributes			Comparative analysis of QOS with Static & Dynamic Ranking	Integrated method of Ranking	Support of Cloud Service models	Ability of QOS Analysis & Micro level prioritization ranking	Complete Coverage of Quality attributes
		Security	Performance	Cost Economy					
QOS ranking prediction model-I	2012	×	✓	×	Static ability of ranking	×	General	×	Limited
QOS ranking prediction model-II	2014	×	×	×	Static ability of ranking	×	General	×	Limited
QOS ranking prediction model-III	2015	×	✓	×	Static & Dynamic ability of ranking	×	General	×	Limited
Cloud Broker/Ranking Algorithm	2016	×	×	✓	Static ability of ranking	×	General	×	Limited
Trust model-TM Ranking	2016	✓	×	×	Static & Dynamic ability of ranking	×	General	×	Limited
Performance based ranking model	2017	×	✓	×	Static ability of ranking	×	SaaS	×	Limited
SPICER-Micro Ranking Algorithm	2017	✓	✓	✓	Both Static and Dynamic ability with Comparative analysis of QOS	✓	SaaS, PaaS & IaaS	✓	Not limited

Conclusion and Future Scope

The Identification the essential quality parameters and method refinements ensures the trust and accuracy of ranking the cloud services. So the major QOS parameters come under the security, performance and cost economy parameters. This is the important key focus areas of cloud services to review and measure the accuracy of ranking them to meet the cloud user expectations. Our model has proposed to provide the complete coverage quality attributes of QOS parameters. The most of the IT related and Bio Applications are more demand among the consumers. The following areas of the bio-technology are cloud computing serves for the vast research and developments. The biomedical information sharing, large-scale Bio-medical and Bio-Technology data management and analysis, Highly sensitive read mapping with Map Reduce for Bioinformatics, Ultrafast and memory-efficient alignment of short DNA sequences to the human genome, Imaging Informatics, Clinical Informatics, Public health informatics, HPC legacy Apps for bio-medical research, Big Data tool based Apps for Genomic Analysis and Computer aided drugs discovery. This SPICER model helps to identify the high quality of applications.

The following survey report ensuring the need of those parameters compared about the past couple of years.



Our model ensures the analysis of service level ranking and user level ranking based on the QOS attributes and user experiences. The scope for the future work is designing and incorporating the SPICER as an Application tool in to the cloud environment is another work proceeded.

References

1. Rizwana Shaikh, Dr. M. Sasikumar. Trust Model for Measuring Security Strength of Cloud Computing Service, International Conference on Advanced Computing Technologies and Applications,Elsevier,2015, PP.380-389.

2. Sahar Abdalla Elmubarak, Adil Yousif, Mohammed Bakri Bashir, Performance based Ranking Model for Cloud SaaS Services,International Journal of Information Technology and Computer Science(ijitcs),2017,PP.65-71.

3. Samir.m.zaid, Hazem.m.elbakry, IIslam.m.abdelhady. A Proposed Framework for Ranking and Reservation of Cloud Services Based on Quality of Service,2015, Vol.3,issue 2.

4. Leyli Mohammadkhanli, Arezoo Jahani. Ranking Approaches for Cloud Computing Services Based on Quality of Service: A Review, ARPN Journal of Systems and Software,2014, Vol. 4, No 2.

5. Vivek Thapar, Dr. O.P. Gupta. Study of Various Parameters of Cloud Computing Environment, International Journal of Application or Innovation in Engineering & Managemen,2016, **Vol. 5, Issue 6**

6. Amid Khatibi Bardsiri, Seyyed Mohsen Hashemi. QoS Metrics for Cloud Computing Services Evaluation, International Journal of Intelligent Systems and Applications (ijisa),2014, PP.27-33.

7. Said Naser, Said Kamil and Nigel Thomas. A Case Study in Inspecting the Cost of Security in Cloud Computing, Electronic Notes in Theoretical Computer Science, 2015, PP. 179–196.

8. Jianhua Chea, Yamin Duanb, Tao Zhanga, Jie Fan, Study on the security models and strategies of cloud computing, International Conference on Power Electronics and Engineering Application, Elsevier,2014, PP.586-593

9. Anup Date, Dinesh Datar. A Multi-Level Security Framework for Cloud Computing, International Journal of Computer Science and Mobile Computing (ijcsmc),2014, PP.528-534.

10. Dhanamma Jagli, Seema Purohit, N. Subash Chandra. Evaluating Service Customizability of SaaS on the Cloud Computing Environment, International Journal of Computer Applications, 2016, Vol. 141, No. 9.

11. Shyam Nandan Kumar, Amit Vajpayee, A Survey on Secure Cloud: Security and Privacy in Cloud Computing, American Journal of Systems and Software, 2016, Vol. 4, No. 1, 14-26.

12. SubramanianAnbazhagan, Dr. K. Somasundaram. A Review on Trust Mechanisms in Cloud Environment, Australian Journal of Basic and Applied Sciences, 2015, PP. 167-175.

13. Devi T, Ganesan R. Platform-as-a-Service (PaaS): Model and Security Issues, TELKOMNIKA Indonesian Journal of Electrical Engineering, 2015, Vol. 15, No. 1, PP. 151-161.

14. Manish Kumar Aery,Sumit Gupta, Comparative study of security parameters by Cloud Providers, Indian Journal of Computer Science and Engineering,2013, Vol. 4 No.2.

15. R. Velumadhava Rao, K. Selvamani. Data Security Challenges and Its Solutions in Cloud Computing International Conference on Intelligent Computing, Communication & Convergence,Elsevier,2015,PP.204-209.

16. G.Ramya, K.Radhika. Personalized QOS based Ranking Approach for Cloud Service Selection, International Journal of Computer Applications,2015, Vol. 127 – No.18.

17. Vivek Shrivastava,D. S. Bhilare. SAFETY: A Framework for Secure IaaS Clouds, International Journal of Advanced

Networking and Applications, 2015 Vol. 06 Issue: 06 PP. 2549-2555.

18. Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, World Congress on Engineering, 2013, Vol II.

19. Gagandeep Kaur, Dr. Mohita Garg, Mrs. Navjot Jyoti, Enhanced Security Mechanism In Cloud Computing: A Review, International Journal Of Computers & Technology,2015, Vol.14, No.6.

20. Mouna Jouini, Latifa Ben Arfa Rabai, Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems, The 6th International Symposium on Frontiers in Ambient and Mobile Systems, Elsevier, 2016, PP.1084-1089.

21. Dhivya .A, Saravanan .M, Cost Based Ranking Service Models in Cloud Computing, International Journal of Advanced Research in Computer and Communication Engineering, 2016 Vol. 5, Issue 3.

22. Vishnu Pratap Singh Kirar. Security Architecture for Cloud Networking: A Survey International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2014, Vol:8, No:12.

23. N.Srujan Kumar Murtaza Ahmed Khan. Linear Programming in Cloud Computing for Practical Outsourcing, Indian Journal of Applied Research 2012, Vol. 2, Issue 2.

24. Narendra Gaurha, Dr.Manish Shrivastava. Data Security in Cloud Computing Using Linear Programming, International Journal of Emerging Technology and Advanced Engineering, 2012,Vol. 2, Issue 7.

25. Nikkita Prakash Jain Dr. D. Y.Patil. Set of Security Parameters for Cloud Computing Storage System, International Journal of Computer Applications, 2015, Vol. 109, No. 14.

26. Shewta Chandage, Vishal S. Patil. CLOUD: Architecture, Security Threats Issues and Countermeasures for Security, International Journal of Advance Research in Computer Science and Management Studies, 2015, Vol. 3, Issue 7.

27. Varuna Upadhyay, Dr. Ashok Jain. An Introduction of Cloud Computing Security and Privacy Issues in IT Industries, International Journal Of Engineering And Computer Science,2015, Vol. 4, Issue 6, PP.12728-12730.

28. Yogita R. Sunwani, Prof. Amit Welekar. Designing Security Method for Cloud Environment Using Attribute Based Signature, International Journal of Engineering Research and General Science, 2015 Vol. 3, Issue 2.

29. Benard O. Osero. Building Scalable Networks on the Cloud based on Network Storage Virtualization Secure Model, Journal of Emerging Trends in Computing and Information Sciences,2015,Vol. 6, No. 7.

30. K. Haripriya, M. Bhasker Rao, B. Ravi Raju. Public Linear Programming Solution For The Design Of Secure And Efficient Computing In Cloud, International Journal of Advanced Computer and Mathematical Sciences, 2012, Vol 3, Issue 4.

31. M. Subha,M. Uthaya Banu. A Survey on QoS Ranking in Cloud Computing, International Journal of Emerging Technology and Advanced Engineering,2014, Vol. 4, Issue 2.

32. Vincent A. Fusaro, Prasad Patil, Erik Gafni,Dennis P. Wall, Peter J. Tonellato. Biomedical Cloud Computing With Amazon Web Services, PLOS Computational Biology, 2011, Vol. 7, Issue 8.

33. Paul Muir, Shantao Li, Shaoke Lou, Daifeng Wang, Daniel J Spakowicz, Leonidas Salichos.The real cost of sequencing: scaling computation to keep pace with data generation, International Journal of Genome Biology, 2016, 17:53.

34. Cloud Security Alliance. "Security Guidance for Critical Areas of Focus in Cloud Computing." Research article, 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

35. Security Guidance for Critical Areas of Focus in Cloud Computing, Research article, v2.1", http://www.cloudsecurityalliance.org

36. Rajkumar Buyya, James Broberg, Andrzej Goscinski. Cloud Computing-Principles And Paradigms, John Wiley & Sons publications,2011. PP.573-590.

37. Barrie Sosinsky, Cloud Computing Bible, Understanding Cloud Security, Chapter 12, Wiley Publishing, 2011.

38. Dan Sullivan. IaaS Providers List: Comparison And Guide, 2014,

39. By Thoran Rodrigues.11 cloud IaaS providers compared, 2012, Alan-pearson. What is Penetration Testing and Why is It is important, 2014, http://www.securityinnovationeurope.com/blog/author/alan-pearson

40. Bonnie Berger, Jian Peng, and Mona Singh, Computational solutions for omics data, NIH public access, 2013, PP 333-346.