Discovering The Trustworthy Cloud Service Provider In Collaborative Cloud Environment

Venisha .A, M.Murali

ABSTRACT--- Cloud computing technology has evolved drastically by adopting superior computing and storage abilities. Cloud computing is perceived as a beneficial option that offers sharing of services across the internet. For storing abundant volume of data, cloud computing can be extremely helpful. The CSP (cloud service provider) finds it challenging to choose a suitable trust model. Moreover, most of the cloud services offer equivalent functionalities though their performances vary as a result selecting suitable cloud service becomes quiet challenging for the user. The cloud service provider provides services to Cloud client in accord with the SLA (Service Level Agreement). The documentation involves, all the transactions that are being classified relying upon the administration type provided by the service provider along with the payment that the client must do. Regrettably, Service Level Agreement isn't taken up seriously, resultant QoS (quality of service) isn't achieved. In various situation, it's observed that reliability is neglected and the administration lacks quality. The present research work attends the issue of choosing the most appropriate CSP (Cloud service provider) that yields high quality. In other words, determining the reliability of CSPs within a cloud environment. Following are the methods involved in the recommended approach 1) Creation of cloud cluster environment 2) Broker creation 3) Machine Agent 4) Feedback Provider and 5) Trust validation. The trust management system incorporates fewer machine agents, feedback gained by utilizing external resources, highly effective in computing trust and CPU's are not left idle or without use. Performance analysis and the output of the experiments prove the efficiency and feasibility of the recommended approach. It's revealed from the output that the proposed methodology offers superior service matching. Using the Trust model, appropriate and specific services can be chosen effectively by the tenants.

Keywords: Cloud computing, Service Level Agreement, Cloud Service Providers, cloud cluster environment, Broker creation, Machine Agent, Feedback Provider and Trust validation.

1. INTRODUCTION

Presently, cloud computing has massively spread its roots by permitting voluminous data storage to external cloud servers, making the process of data storage scalable. Offering data security stands as one of the major concern in cloud computing. Today it's quite simple for the malicious users to get access to the stored data. Usually in a cloud storage environment, data files and records that are valuable are handles by a third party, making data security factor as a prime concern within the cloud domain. Clients or customers data is usually stored in cloud which can be accessed via multiple resources that are being connected and distributed. Safety and security of this stored data is highly essential for offering secure communication across the cloud environment. Though there exist numerous advantages delivered by the cloud computing that includes, dynamic virtualized resources, minimizing cost, storage of voluminous data and enhanced productivity, on the other hand it attracts the issue of security threats too. The various sorts of attacks includes: DoS (denial-of-service), authentication attack and worms' injection attack [1]. Merely on the basis of assurance, one cannot determine trustworthy CSPs within a cloud environment. The present research work attends the issue of choosing the most appropriate CSP (Cloud service provider) that yields high quality. To achieve this, the work incorporates the approach of trust validation that is being employed. The work recommends selection of trustworthy CSP relying upon the broker agent into machine agent. Following are the methods involved in the recommended approach, 1) Creation of cloud cluster environment 2) Broker creation 3) Machine Agent 4) Feedback Provider and 5) Trust validation. It's proposed to employ low overhead trust computing by making use of less no: of agents towards the broker end along with employing feedback mechanism for raising efficiency. The research resolves the issue of trust management within a multi-cloud scenario by relying upon a group of distributed TSPs (Trust Service Providers). TSPs are considered as independent third-party providers that offers trust based services to cloud participants and which are being completely trusted by CPs, CSPs as well as CSUs (Cloud Service Users). The information related to the obedience of a service provider in terms of SLA (Service Level Agreement) and the Cloud Service Users feedback helps in assessing the objective and a subjective trust of cloud service providers. There exists an interaction amidst the Machine agent via trust propagation network which allows feedback porkers to gain trust information related to a CSP from rest of the feedback providers. Eventually, the process of trust validation determines the blacklisted ip, detects users that are unauthorized, verifies suitable request parameters and utilizes decision tree algorithm for assessing trustworthy CSPs. It's revealed from the output that the proposed approach yields effectiveness and stability in distinguishing amidst trustworthy and untrustworthy cloud service providers.

Revised Manuscript Received on December 22, 2018.

Venisha .A, Department of Computer Science and Engineering,SRM Institute of Science and Technology, Kattankulathur

Dr.M.Murali, Department of Computer Science and Engineering,SRM Institute of Science and Technology, Kattankulathur

Following is the classification of the journal. Section 2 presents a brief work of previous author. Section 3 illustrates recommended machine learning techniques and the aspects of various levels. Section 4 illustrates experimental outcome. And Section 5 presents the conclusion of the research work along with proposing research work for future.

2. RELATED WORK

Xiaoyong Li, put forth T-broker which being a trust aware service brokering approach for effective matching cloud services/resources that aids in fluffing multiple user requests. Herein proposed a third party-based service brokering architecture concerning multiple cloud environments wherein the T-broker resembles the middleware between the cloud trust management and service matching. It's revealed that T-broker produces better output in various situations also the recommended handles different dynamic service behaviors from multiple cloud sites in a robust manner [2].

Haiying Shen et.al presents 'Harmony', an integrated resource/reputation management platform, that aids in collaborative cloud computing. The multi-QoS-oriented resource selection component aids the requesters in selecting resource providers which provides highest QoS evaluated by the requesters' priority consideration of multiple-QoS attributes. Nodes offering maximum QoS while delivering resources are being given incentives by the price-assisted resource/ reputation control component. Moreover, it aids the providers in maintaining high reputations and preventing from getting overloaded during increasing their incomes. When the components work together, reliability and efficiency of sharing distributed resources can be made better that are scattered globally across CCC [3].

Hamid Mohammadi Fard et.al, proposes a pricing model and a truthful mechanism in order to schedule single tasks by incorporating two objectives which being the monetary cost and completion time. Truthfulness and the efficiency of the mechanism is being examined theoretically thereby depicting intense experimental output that reveals remarkable effect of the mean/self-centered conduct portrayed by the Cloud providers concerning efficiency of the entire system. The experiments are carried out based on real-world and synthetic workflow applications which illustrates that the proposed solutions mostly lead over the Pareto optimal solutions assessed by the two conventional multi-objective evolutionary algorithms [4].

Fawaz Paraiso et.al, attends such concerns by presenting the federated multi-cloud PaaS infrastructure. This infrastructure relies upon basic three foundations: 1) an open service model deployed for designing and implementing multi-cloud PaaS as well as the SaaS applications executing on top of it, 2) a configurable architecture of the federated PaaS, and 3) few infrastructure services in order to manage multi-cloud PaaS as well as the SaaS applications. Thereafter, illustrating the deployment of multi-cloud PaaS on top of thirteen prevailing IaaS/PaaS. Eventually, reporting of 3 distributed SaaS applications built and implemented over the federated multi-cloud PaaS infrastructure [5].

Ismail Butun et.al, recommends theservice approach of cloud-centric multi-level authentication for the responder devices. The prime focus is to build a cloud-centric public safety network that assures to be both reliable and resilient. The Cyber-physical system being such a network which provides complete integration of the cyber and physical components (that is computing, sensing, control, and networking). Hence, in order to build a reliable public safety network, security and privacy must be framed during design [6].

Ms. R. Parameswari et.al, presents that Trust Networks evolves from two viewpoints: first being that the user acts as the one and only 'lifelong' gamut across the Trust Networks and that the scope & variety of the Trust Networks revolves around the users' well-being. The second viewpoint being from the service providers' side where two orthogonal axis or attraction pools are focused that is regional development and other being interests & communality. Though the research perceives a bottom-up mechanism that is initiating with reference cases that being smaller and local, but the governments overlook the outcome and rather potentially huge national rollouts, involving inter-linking of multiple trust networks into Trust Ecosystems. Moreover, the Trust Ecosystem level tends to be the target of the TAS3 project guiding principles, standards & methods, fostering them towards new candidate TN [7].

Canh Ngo et.al, recommends the approach of Dynamic Trust Establishment that is being deployed into cloud services provisioning life-cycles concerning the multi-provider Inter cloud environment. For the purpose of trust evaluation and delegation, it usually depends on attribute-based policies. The research recommends a mechanism that can be practical deployed for the assessment of attribute-based policies by making use of Multi-type Interval Decision Diagrams extended from Integer Decision Diagrams that being highly effective with respect to evaluation complexity compared to rest of the evaluation approaches [8].

Nivethitha Somu et al, presents that in a cloud marketplace, with the large number of prevailing CSPs (Cloud Service Providers), selecting the most suitable and desired CSP becomes quite challenging for the CUs (Cloud Users).With the aid of an appropriate service selection framework, the users can opt out for the desired CSP, at the same time encouraging the CSPs to fulfill or abide by the SLA (Service Level Agreement) thereby improvising the QoS (Quality of Service). Though the algorithms of arithmetic residue and EM (Expectation–Maximization) are deployed for determining missing values, they don't exhibit to be appropriate. [9].

PeiYun Zhang et.al Cloud computing has evolved as one of the demanding and important scientific computing as well as commercial application paradigm where in multiple computing resources and data resides within the clouds that can be shared, though simultaneously it confronts many trust issues. A new trust model and relevant algorithm is being proposed for minimizing trust management overhead and

enhancing the power of malicious node detection by relying upon the domain partition. The disadvantage being that it lacks confidentiality [10].

Jirayu Kanpariyasoontorn et al, discusses that deployment of Cloud computing is at a large scale by the corporate personnel. With the existence of multiple CSPs that offer almost equivalent services, the QoS (quality of service) stands out to be an essential factor for selecting best suitable cloud service. Herein proposes a trustworthiness assessment method that relies upon the CSA Cloud Controls Matrix security NIST SP800-53 Consensus. There is an evaluation of the Assessments Initiative Questionnaire for computing the trustworthiness score of the service. By using the assessment method and comparing trustworthiness of candidate cloud service, the client/consumer is guided, though there is an issue of reliability [11].

Matin Chiregi et.al, put forwards that the trust and reputation in cloud computing are projected in case sufficient services and expectations have been achieved. The reputation values are assessed by the design and the trusted services within the cloud are determined by the means of accessibility, ability and dependability. A method is recommended for the trusted service by employing 3 topological measures, which being in-degree, out-degree and reputation measures. It's elucidated from the output that on the basis of TSPs suggestion, there is an increase in the accuracy but actually there is less accuracy gained [12].

Erdal Cayirci1 et.al, presents the joint trust and risk model for federated cloud services. The proposed model relies upon the CSPs performance history. Addresses aleatery uncertainty via probability distributions and static stochastic simulation analytical insight into the model has been offered via numerical analysis through Monte-Carlo simulation. Though minimum security is achieved [13].

M. H. Ghahramani et.al, Cloud is being referred to as a novel computing paradigm that offers the users/consumers/clients with on-demand, scalable and virtual resources. Without any strenuous administrative efforts the users can easily get access to a large volume of shared computing resources. A detailed survey is being performed on the proposed models in accord with the implementation principles for attending the concerns related to QoS guarantee and dependability [14].

Xianrong Zheng et.al discusses that in recent years cloud computing has widely spread its roots. Usually the CSPs compete among each other for offering equivalent services across the Internet. The QoS (Quality of service) factor tends to be a significant differentiator amidst CSPs that offer similar services. It (QoS) specifies how efficiently a service is carried out thereby aiding the CSP to highlight their services, and assisting the cloud consumers to find out the services that matched their QoS expectations. In addition an approach of collaborative filtering is being proposed by employing Spearman coefficient for suggesting cloud services. Both QoS ratings as well as rankings for cloud services can be predicted by imbibing this approach though scalability achieved is not as desired [15].

Hadeel T. El Kassabi et.al, discusses that there is a massive evolution of Cloud computing which aids in offering data-intensive services across the Internet and involves abundant generation of data via multiple sources. There usually lack trust issues. AMDTM (multi-dimensional trust model) is being recommended for the processing of Big Data workflow across multiple clouds that assesses the CSP trustworthiness depending on: highly up-to date cloud resource capabilities, the reputation proof computed by the neighboring users and a recorded experience of personal history with the cloud provider, though dynamicity is not assured [16].

Sarbjeet Singh et.al, states that trustworthiness resembles the compliance degree of a CSP to the assured quantitative QoS factors as listed in the SLA. Since there prevails numerous CSPs providing equivalent services within the cloud environment, its quiet tough for the cloud users/clients to select best trustworthy CSP. As a solution, herein proposed a CMTES (Compliance-based Multi-dimensional Trust Evaluation System) which aids the clients in determining the CSPs trustworthiness from various angles. It's elucidated from the output that the proposed approach of CMTES is stable and distinguishes amidst trustworthy and untrustworthy CSPs effectively. The demerit being that integrity is low [17].

Talal H. Noor et.al, discuses that for the advancement and acceptance of cloud computing, the prime concern is of Trust management. Maintaining the consumer/clients privacy is indeed challenging as the communication information amidst the consumers and the trust management service is highly sensitive. Herein elaborated the design and deployment of Cloud Armor which being a reputation-based trust management framework, offering a set of functionalities by delivering TaaS (trust as a service), but confronting low scalability and dependability [18].

Zheng et.al, have recommends a thorough study to offer precise QoS ranking for cloud services. Nevertheless, ranking-oriented methods are deployed for selecting optimal cloud service amidst a set of functionally equivalent cloud services, such methods avoid any change of QoS. For predicting missing QoS values both the rating-oriented collaborative filtering methods as well as ranking-oriented collaborative filtering methods tends to be helpful for the user, though they avoid considering the dynamic QoS properties in MCC. Resultant it suffers from rating fraud detected [19].

Rajendran and Swamynathan recommends a combinatorial model for assessing trust dynamism in the cloud services. Using the feedback of the cooperative user, there pupation can be computed. Basically, feedback rating resembles outlook of every user concerning the interested services. Exposed services that successfully satisfy the requirements of the users are ranked based on their trust value, thereafter the top-k cloud services are being recommended to the user. Though it offers reliability, security and dynamicity, it confronts low safety, dependability and confidentiality [20].

Also, Char band et.al, recommends a novel method by deploying feedback assessment component and Bayesian game model to determine unreal/fake feedback in the cloud trust management systems. These two proposed methods of

feedback assessment component and the Bayesian game model helps in determining fake feedbacks. Though it offers better reliability and security, but confronts low scalability and dependability [21].

Hanna M. Said et.al put forth the performance of machine learning (ML) techniques deployed in attack identification within a cloud environment. For the final selection of a learning technique for the task, statistical ranking approach is being incorporated. There is an assessment of C4.5 technique's performance via multiple performance evaluation matrices, involving rigorous testing of 10-fold cross-validation, true and false positive rate, recall, precision, F-measure and the area of receiver operating characteristic [22].

3. PROPOSED WORK

3.1 Overview

Cloud computing has evolved as one of the demanding and important scientific computing as well as commercial application paradigm where in multiple computing resources and data resides within the clouds that can be shared, though simultaneously it confronts many trust issues. There exist malicious providers that offer low graded services to the users, also malicious users may offer good providers false trust validation. Moreover, the CSP stores the customer data, permitting a restrictive control to the consumer over handling of its data. Though former work presents selection of trustworthy CSPs, they confront certain challenges in performing so. The prime concern is building and retaining trust in the cloud service. The proposed approach makes use of less no: of agents towards the broker end along with employing feedback mechanism for raising efficiency. The broker employs the machine agent code. By the means of performance analysis and experimental outcome, feasibility and effectiveness can be validated. Within the cloud environment, trusted cloud computing can be initiated involving the associated actors. The trust management system incorporates fewer machine agents, feedback gained by utilizing external resources, highly effective in computing trust and CPU's are not left idle or without use.

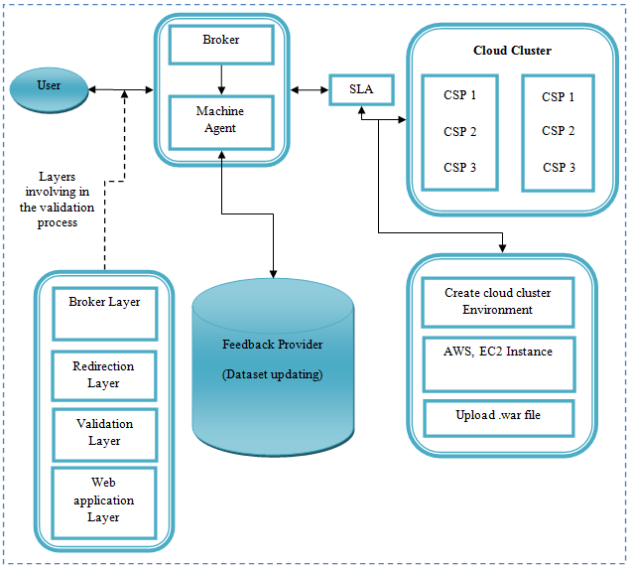

Figure 1: Overall Architecture

3.2 Cluster Environment

Cluster resembles an assembly of various server instances, covering greater than one node, all executing with same configuration. AWS resembles a CSP (cloud service provider). This service being apt example of actual cloud computing. Account is being generated in AWS and EC2 for launching few or lot of virtual servers according to requirement. In EC2 clusters are built thereby employing the application in EC2 cluster.

3.3 Broker Creation

With the availability of numerous public and private CSPs, there occurred the need of CSBs (Cloud Service Brokers), and for the necessity of handling the utilization of those services in an enterprise. Broker aids in providing services ranging from storage, application, computation, database, etc. depending on the incoming request from a consumer. In general, Cloud broker resembles service discovery, intermediation and aggregation'. The Broker application behaves as a platform amidst client and machine agent and is utilized in AWS instance. It incorporates the machine agent rule which more or less resembles a proxy.

3.4 Machine Agent

Machine agent resembles a software entity and resembles an independent software program that executes instead of the network user. These agents perform in an environment that is dynamically changing. The agents basically communicate among each other, exchange information and collaboratively carry out complicated tasks. They handle sever management and specifies rules to the broker application concerning security, these includes: SQL injection, DDoS (Denial of service), blacklisted IP and Flooding attack.

3.5 Feedback Provider

Trust offers a rating /reputation based feedback mechanism that being a significant reference for various users. For various cloud environments, dependability of a feedback-mechanism stands highly significant. There may exist numerous malicious users in an open cloud environment and their ratings can result in misleading and false output. With the Feedback provider frequent blacklist IP and white list IP can be detected by utilizing abnormal text in request form and permitting or granting access to only authenticated users.

3.6 Trust Validation

The trust mechanism is an effective approach for enhancing the security parameter in a cloud environment. As stated the prime concern or challenge is inadequate trust amidst the users and CSPs. Hence for building a safe and secure cloud environment, trust is highly essential. Trust basically resembles a cordial relation amidst two parties that perform reliably, securely and dependably in any situation for a given time period. Trust validation employs decision tree (DT) algorithm where in verification of actual request parameters is done alongside blacklisted IP and

unauthorized users are identified. As a result this trust computing scheme assures to be highly appropriate for large-scale cloud computing scenario.

3.7 Decision Tree Algorithm

The decision tree algorithm works in different levels. At every level an attribute is utilized for building new cloud service providers in the decision tree. Once CSPs are generated, the selected service providers with few records of training dataset denotes end of a level/step. The process carries on alternatively in various steps for the rest of the data and CSP still the tree is built completely.

Training data=(x1, x2….)
While CSP Number>0 do
For each cloud service provider CSPi Do
Sorted data =Sort Training Data by (CSPi)
CSP Trust [i]=Define Trust (CSPi, Sorted data)
End for
Selected CSPs=Compare Trust (CSPs Trust)
Extract CSP=Determine CSP (Selected Trustworthy CSPs)
Estimated Accuracy (Determine CSP)
End While

4. RESULT AND DISCUSSION

Employing various techniques for data security proves extremely beneficial and contributed remarkably in providing security within a Cloud computing environment. The existing work elaborates security relying upon trustworthy CSP in cloud computing. Moreover, the study review illustrates that further improvisation can be carried out in the trust validation of CSP. For fetching of hidden attributes, appropriate methods needs to be developed from the datasets. But such a process tends to be tedious as the cloud computing datasets possess in consistent attributes. The research deploys DT (decision tree) algorithm for the identification of trustworthy CSP.

Table 1 depicts comparison of proposed Decision tree (DT) algorithm. It represents security performance and comparison results in contrast to various prevailing techniques such as T-broker, MLP (Multi-Layer Perceptron) and SVM (Support Vector Machine). The proposed DT algorithm yields in better output in comparison to rest of the algorithms. Also the work determines throughout performance in terms of accuracy and time.

Table 1: Comparison of Techniques based on Security

S.No	Techniques	Security
1	T-Broker	87
2	Multi layer Perceptron (MLP)	92.38
3	Support vector machine(SVM)	89.2
4	Decision Tree(DT)	92.5

Fig 2: Comparison of performance security analysis techniques

The Figure 2 depicts comparison of proposed Decision tree (DT) algorithm. It represents security performance and comparison results in contrast to various prevailing techniques such as T-broker, MLP (Multi-Layer Perceptron) and SVM (Support Vector Machine). The proposed DT algorithm yields in better output in comparison to rest of the algorithms.

Table 2 depicts comparison of proposed Decision tree (DT) algorithm. It represents accuracy, time-performance and comparison results in contrast to various prevailing techniques such as T-broker, MLP (Multi-Layer Perceptron) and SVM (Support Vector Machine). The proposed DT algorithm yields in better output in comparison to rest of the algorithms. Also the work determines throughout performance in terms of accuracy and time.

Table 2: Comparison of Techniques in based on Accuracy and Time

S. No	Techniques	Accuracy (%)	Time (ms)
1	T-Broker	80	0.84
2	Multi layer Perceptron (MLP)	92	0.75
3	Support Vector Machine(SVM)	92.45	0.67
4	Decision Tree(DT)	95	0.57

Fig 3: Comparison of Accuracy and Time analysis

The Figure 3 depicts comparison of proposed Decision tree (DT) algorithm. It represents accuracy, time-performance and comparison results in contrast to various prevailing techniques such as T-broker, MLP (Multi-Layer Perceptron) and SVM (Support Vector Machine). The proposed DT algorithm yields in better output in comparison to rest of the algorithms.

5. CONCLUSION

In recent years cloud computing has widely spread its roots. Usually the CSPs compete among each other for offering equivalent services across the Internet along with confronting various security issues. The QoS (Quality of service) factor tends to be a significant differentiator amidst CSPs that offer similar services. The present research work offers highly energy efficient way for selecting the best trustworthy CSP (cloud service provider for CUs (cloud users). The trust management system incorporates fewer machine agents, feedback gained by utilizing external resources, highly effective in computing trust and CPU's are not left idle or without use. It's elucidated that the proposed methods yields in high accuracy by employing the suggestion of the trusted service.

REFERENCES

1 Hasan Mahmoud Kanaker, Madihah Mohd Saudi, Mohd Fadzli Marhusin "Detecting worm attacks in cloud computing environment: proof of concept", © IEEE 5th Control and System Graduate Research Colloquium, 2014, p.p. 253 – 256.
2 Xiaoyong Li, Huadong Ma, Feng Zhou, and Wenbin Yao "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 7, 2015, P.P. 1402-1415.
3 Haiying Shen and Guoxin Liu "An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 4, 2014, p.p. 862-875.
4 Hamid Mohammadi Fard, Radu Prodan and Thomas Fahringer "A Truthful Dynamic Workflow Scheduling Mechanism for Commercial Multi-Cloud Environments", © IEEE Transactions On Parallel And Distributed Systems, 2012, P.P. 1-10.

5 Fawaz Paraiso, Nicolas Haderer, Philippe Merle, Romain Rouvoy, Lionel Seinturier "A Federated Multi-Cloud PaaS Infrastructure", © IEEE Fifth International Conference on Cloud Computing, 2012, p.p. 392-399.

6 Ismail Butun, Melike Erol-Kantarci, Burak Kantarci, and Houbing Song "Cloud-Centric Multi-Level Authentication as a Service for Secure Public Safety Device Networks", ©IEEE, Critical Communications and Public Safety Networks, 2016, p.p. 47-53.

7 R. Parameswari, Ms.G.C.Priya and Dr.N.Prabakaran "A Trust, Privacy and Security Infrastructure for the Inter-Cloud", IJCTA, Vol. 3, 2012, p.p. 691-695.

8 Canh Ngo, Yuri Demchenko, Cees de Laat "Toward a Dynamic Trust Establishment Approach for Multi-provider Inter cloud Environment", © IEEE 4th International Conference on Cloud Computing Technology and Science, 2012, p.p. 532-538.

9 Nivethitha Somu, Kannan Kirthivasan, Shankar Sriram V.S. "A computational model for ranking cloud service providers using hypergraph based techniques", © Elsevier B.V. All rights reserved, Future Generation Computer Systems Vol. 68, 2017, p.p. 14–30.

10 PeiYun Zhang, Yang Kong, and MengChu Zhou, "A domain partion based trust model for unreliable cloud" © IEEE, 2018, p.p.2167-2178.

11 Jirayu Kanpariyasoontorn, Twittie Senivongse., "Cloud Service Trustworthiness Assessment Based on Cloud Controls Matrix", ICACT, 2017, p.p. 291-297.

12 Matin Chiregi, Nima Jafari Navimipour, "Trusted services identification in the cloud environment using the topological metric", © Elsevier, Karbala International Journal of Modern Science 2 © 2016, p.p. 203-210.

13 Erdal Cayirci, Anderson Santana de Oliveira, "Modelling trust and risk for cloud services", © Cayirci and de Oliveira Journal of Cloud Computing: Advances, Systems and Applications, 2018.

14 M. H. Ghahramani, Meng Chu Zhou, Chi Tin Hon, "Toward Cloud Computing QoS Architecture: Analysis of Cloud Systems and Cloud Services", IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 1, p.p. 6 – 18, 2017.

15 Xianrong Zheng, Li Da Xu, Sheng Chai, "QoS Recommendation in Cloud Services", © IEEE, 2017p.p. 5171-5176.

16 Hadeel T. El Kassabi, Mohamed Adel Serhani, Rachida Dssouli1 and Boualem Benatallah "A Multi-Dimensional Trust Model for Processing Big Data over Competing Clouds", © IEEE, 2017, p.p.1-18.

17 Sarbjeet Singh, Jagpreet Sidhu, "Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers", © Elsevier, 2016, p.p. 109-132.

18 Talal H. NoorQuan Z. ShengLina Yao. Schahram Dustdar, Anne H.H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services", © IEEE, 2016, p.p. 367-380.

19 Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS ranking prediction for cloud services," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 6, pp. 1213–1222.

20 Rajendran V.V, Swamynathan.S "Hybrid model for dynamic evaluation of trust in cloud services", Wirel.Netw., 2015, p.p. 1–12.

21 Charband.Y, Navimipour.N.J "Online knowledge sharing mechanisms: a systematic review of the state of the art literature and recommendations for future research" Inf. Syst.Front. 2016, p.p. 1–21.

22 Hanna M. Said, Ibrahim El Emary, Bader A. Alyoubi, Adel A. Alyoubi "Application of Intelligent Data Mining Approach in Securing the Cloud Computing", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7, No. 9, 2016, p.p. 151-159.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication