IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-04, Issue-02 E-ISSN: 2347-2693

A Survey on Emergence of Cloud Computing Using Brokering Services

B. Mahesh kumar[1*] and V.Savitha[2]
[1*,2] Department of Computer Science and Engineering, Anna University ,Chennai, India
www.ijcseonline.org

Received: Jan /21/2016 Revised: Feb/04/2016 Accepted: Feb/15/2016 Accepted: Feb/29/2016

***Abstract*—**Trust management is very crucial aspect in multiple cloud environment .To ensure this Trust-management. Our paper presents C-provider, a trust aware brokering scheme for managing efficient cloud resources (or) services. The C-provider is based on a third party brokering architecture that is proposed to act as a middleware for cloud management and service matching.Our C-provider uses a hybrid and adaptive trust model to compute the overalltrust degree of resources based on the monitored feedbackof the service resources. Also C-provider uses a minimal feedback mechanism that effectively reduces networking issue and improve system efficiency.

***Index Terms*—** Multiple Cloud Computing, Trust-Aware Servicebrokering, Resource Matching, Feedback Aggregation

I. INTRODUCTION

Multiple cloud theories and technologies are the hot directions in the cloud computing industry, which a lot of companies and government are putting much concernto make sure that they have benefited from this new innovation [1], [2]. However, compared with traditional networks, multiple cloud computing environment has manyunique features such as resources belonging to each cloud provider, and such resources being completely distributed, heterogeneous, and totally virtualized; these features indicate that unmodified traditional trust mechanisms can no longer be used in multiple cloud computing environments. A lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services [3], [4]. Thus, the development of trust awareness technology for cloud computing has become a key and urgent research direction [5]–[8]. Today, the problem of trusted cloud computing has become a paramount concern for most users. It's not that the users don't trust cloud computing's capabilities; rather, they mainly question the cloud comput-ing's trustworthiness [9]–[11].

A. Motivation

The emergence of cloud brokers acting as an intermediary between cloud providers and users to negotiate and allocate resources among multiple sites. Unfortunately, apart from OPTIMIS [12], most of these brokers do not provide trust management capabilities for multiple cloud collaborative computing, such as how to select the optimal cloud resources to deploy a service, how to optimally distribute the different components of a service among different clouds, or even when to move a given service component from a cloud to another to satisfy some optimization criteria.From many scholars understanding [6]–[11], [13], [14], [17], to increase the adoption of cloud services, cloud providers must first establish trust to alleviate the worries of a large number of users [25]. To manage and schedule resources with high trustworthy, we need an accurate way of measuring and predicting usage patterns of computing resources whose patterns are changing dynamically overtime. From here, the main motivation of this paper is to construct a trust-aware service brokering system for efficient matching computing resources to satisfy various user requests.

Although several scholars have been attracted by this question and carried out some studies [7]–[9], [13], [14], [17], their methods have not been able to breakthrough the existingideas in previous trust models [15], [16], 25]. First, some hybrid trust models are proposed for cloud computing environment (see [13], [14]). It is no doubt that how to adaptively fuse direct trust (first-hand trust) and indirect trust (users' feedback) should be an important problem, however, most current studies in hybrid trust models either ignore the problem or using subjective or manual methods to assign weight to this two trust factors (first-hand trust and users' feedback) (see [13], [14]). This may lead to misinformation and preclude an accurate evaluation of trustworthiness. At the same time, evidence-based trust evaluation can reflects real-time behavior of service providers [7], [9], and it should be a process of multi-attribute decision-making. Avoiding the effect of individual favouritism on the weight allocation of trust indicators is a key task. However, most previous studies used subjective methods to weight the trust indicators (see [7], [9]). Their approaches do not reflect trust decision-making adaptability, and may lead to deviation from objective facts. Furthermore, consider industry data centers, which host hundreds of machines and handles thousands of request per second, the delay induced by trust system can be one big

problem. There is no doubt that the efficiency of a trust system is an important requirement for multiple cloud environment. That is, the trust brokering system should be fast convergence and light-weight to serve for a large number of users and providers. However, existing studies paid little attention to this question, which greatly affects scalability and availability of the trust system (see [14], [25]).

- C-provider uses a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining dynamic service behavior with the social feedback of the service resources.

- C-provider uses a maximizing deviation method to compute the direct trust of service resource, which can overcome the limitations of traditional trust models, in which the trusted attributes are weighted manually or subjectively. At the same time, this method has a faster convergence than other existing approaches.

These innovative designs and other specific features (e.g., real-time trust degree calculation approach based on time attenuation function and lightweight feedback mechanism) collectively make C-provider an efficient solution that can beused in multi-cloud environment. The experimental results show that, compared with the existing approaches, our C-provider yields very good results in many typical cases, and the proposed system is robust to deal with various numbers of dynamic service behavior from multiple cloud sites.

The remaining parts of this paper are organized as follows: Section II gives an overview of related work. C-provider's architecture is described in Section III. Section IV outlines the details of the trust calculation mechanism. The experi-mental results are presented in Section V. Finally, Section VI concludes the paper and suggests future directions.

II. RELATED WORK

The main contributions of our trust scheme are based on many existing representative work. In this section, we first review the typical work of cloud brokers. We then analyze the developments of trust management in cloud computing.

A. Development of Cloud Brokers

In recent years, there are many cloud service brokers or monitoring systems emerged as a promising concept to offer enhanced service delivery over large-scale cloud environments. Some private companies offer brokering solutions for the current cloud market, e.g., RightScale [20] or SpotCloud [21].

In [18], the authors use the Lattice monitoring framework as a real-time feed for the management of a service cloud. Monitoring is a fundamental aspect of Future Internet elements, and in particular for service clouds, where it is used for both the infrastructure and service management. The authors present the issues relating to the management of service clouds, discussing the key design requirements and how these are addressed in the RESERVOIR project [18]. The authors also present the Lattice monitoring framework, discussing its main features and also giving an overview of its design and implementation, together with a presentation of its use within RESERVOIR.

In [19], the authors point out, although many solutions are now available, cloud management and monitoring tech-nology has not kept pace, partially because of the lack of open source solutions. To address this limitation, the authors describe their experience with a private cloud, and discuss the design and implementation of a private cloud monitoring system (PCMONS) and its application via a case study for the proposed architecture. An important finding of this work is that it is possible to deploy a private cloud within the organization using only open source solutions and integrating with traditional tools like Nagios. However, there is significant development work to be done while integrating these tools.

RightScale [20] is a web based cloud computing managing tool for managing cloud infrastructure from multiple providers. RightScale enables organizations to easily deploy and manage business-critical applications across public, private, and hybrid clouds. SpotCloud [21] provides a structured cloud capacity marketplace where service providers sell the extra capacity they have and the buyers can take advantage of cheap rates selecting the best service provider at each moment. The broker in [24] also provides this feature but in an automatized way,without checking manually the prices of each cloud provider at each moment. Thus, optimization algorithms can be used to select the best way to place the VM according to the actual rates of the cloud providers.

Aeolus [22] is an open source cloud management software sponsored by Red Hat, which runs on Linux systems. It provides both ease the burden of managing large numbers of clouds, as well as ensure that cloud consumers can use large numbers of clouds to avoid getting locked into the offering of any single provider. Besides managing virtual machines in various clouds, a cross-cloud broker like Aeolus needs to be able to build images for these clouds from a single specification, track that images have been converted and uploaded into what cloud, as well as automate image updates. To further simplify the management of complicated cloud uses, Aeolus makes it possible to describe multi-instance applications like three-tier web applications as one unit, from image definition to

upload and launch into target clouds. The main components of Aeolus are Conductor, the application that users and administrators interact with, Composer, an application and tools for building and managing images, and Orchestrator, tooling for treating groups of virtual machines as one application.

According to the Cloud Security Alliance's work, a cloud is modeled in seven layers: Facility, network, hardware, OS, middle ware, application, and the user. These layers can be controlled by either the cloud provider or the cloud customer. In [23], the author presents a set of recommended restrictions and audits to facilitate cloud security. The author found, although the recommendations might be overkill for deploy-ments involving no sensitive data, they might be insufficient to allow certain information to be hosted in any public or community cloud.

EU project OPTIMIS has addressed the trust brokering problem for multiple clouds and a full-fledged OPTIMIS toolkit is available for the developers at present [12]. OPTIMIS can identify, capture and codify what an optimized cloud ecosystem driven by trust, risk, eco-efficiency and cost will look like. The OPTIMIS framework and toolkit will simplify service construction, and support deployment and runtime decisions based on prior evaluation of providers. OPTIMIS deliverables can enable clouds to be composed from multiple services and resources. It will support service brokerage via interoperability, and is architecture-independent.

B. Trust in Cloud Computing

Several research groups both in academia and industry are working in the area of trust management in cloud computing environment. This section will take an in-depth look at the recent developments in this area.Khan et al. have reviewed the trust needs in the cloud system [5]. They analyze the issues of trust from what a cloud user would expect with respect to their data in terms of security and privacy. They further discuss that what kind of strategy the service providers may undertake to enhance the trust of the user in cloud services and providers. They have identified control, ownership, prevention and security as
the key aspects that decide users' level of trust on services. Diminishing control and lack of transparency have identified as the issues that diminishes the user's trust on cloud systems. The authors have predicted that remote access control facilities for resources of the users, transparency with respect to cloud providers actions in the form of automatic traceability facili-ties, certification of cloud security properties and capabilities through an independent certification authority and providing security enclave for users could be used to enhance the trust of users in the services.

Hwang and Li suggested using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners [6]. The authors build reputation systems using a Distributed-hash-table (DHT)-based trust-overlay networks among virtualized data centers and distributed file systems. These networks over cloud resources provisioned from multiple data centers for trust management and distributed security enforcement. Data coloring and software watermark-ing techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds. In [25], Hwang and Kulkarni also presented an integrated cloud architecture to reinforce the security and privacy in cloud applications. They propose an approach to integrating virtual clusters, security-reinforced datacenters, and trusted data accesses guided by reputation systems. However, in [6] and [25], the authors only focused on the trust and privacy issues of user-side, and they did not mention about server-side trust problem.

Kim et al. present a trust model for allocation of resources to satisfy various user requests [7]. Their trust model collects and analyzes reliability based on historical information of servers in a Cloud data center. Then their trust model prepares the best available resources for each service request in advance, and provide the best resources to users.

Fan and Perros propose a trust management framework for nulti-cloud environments [13], they address the problem of trust management in multi-cloud environments using a trust management architecture based on a group of distributed Trust Service Providers (TSPs). The proposed trust management framework for a multi-cloud environment is based on the proposed trust evaluation model and the trust propagation network. However, in [13], direct trust evaluation still use traditional subjective Probability method, rather than direct service behavior. How to adaptively fuse indirect trust and direct trust, this paper did not discuss in detail.

Ghosh et al. propose SelCSP: a framework to facilitate selection of cloud service providers [14]. It combines trust-worthiness and competence to estimate risk of interaction. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on trans-parency in providers SLA guarantees. However, in SelCSP, trust evaluation still use traditional subjective ratings, rather than real-time service behavior.Habib et al. propose a trust-aware framework to verify the security controls considering consumers' requirements [15]. The authors model the security controls in the form of trust

properties. Then, they introduce a taxonomy of these properties based on their semantics and identify the authorities who can validate the properties. The taxonomy of these properties is the basis of trust formalisation in their proposed framework. Furthermore, a decision model is proposed as an integral part of the framework in order to empower consumers to determine trustworthiness of cloud providers. In [15], trust evaluation still is subjective method based on ratings.

Nagarajan and Varadharajan propose TESM: a trust enhanced secure model for trusted computing platforms [16]. The authors argue that given the nature of both binary and property based attestation mechanisms, an attestation requester cannot be absolutely certain if an attesting platform will behave as it is expected to behave. TESM uses a hybrid trust model based on subjective logic to combine 'hard' trust from measurements and properties and 'soft' trust from past expe-riences and recommendations to reduce such uncertainties. However, how to fuse these trust factors, e.g., hard trust or soft trust, this paper also did not discuss in detail.Noor and Sheng propose the "Trust as a Service" (TaaS) framework to improve ways on trust management in cloud environments [17].

In particular, the authors introduce an adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks. However, this framework does not allow to assess trustworthiness based on monitoring information as well as users' feedback.In the author's previous research [10], based on technology of distributed agents, trusted cloud service architecture is suggested for efficient scheduling cloud resources satisfying.

Figure-1

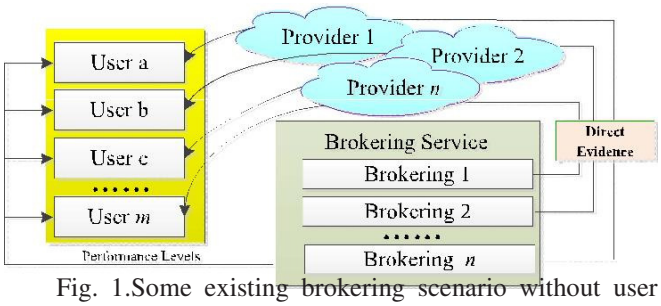


Fig. 1.Some existing brokering scenario without user feedback.

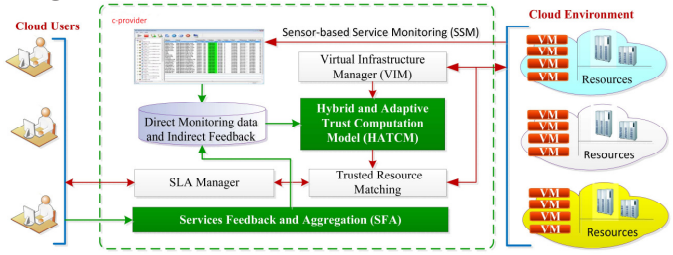
various user requests. The cloud service architecture aims to monitor servers dynamically and allocate high quality computing resources to users. The trusted data acquisition mechanism in this paper uses the monitored information of nodes in the cloud environment. This information consists of each node's spec information, resources usage, and response time. Then the model analyzes this information and prepares suitable resources on each occasion, and then allocates them immediately when user requests. As a result, cloud system can provide the high trustworthiness resources and high-level services based on the analyzed information and it is possible to utilize resources efficiently. In a recent work [11], the authors proposes a service operator-aware trust scheme (SOTS) for resource matchmaking across multiple clouds. However, both [10] and [11] only consider direct monitoring information without the user feedback information.

III. C-PROVIDERARCHITECTURE

As mentioned in Part A of Section I, most current cloud brokering systems do not provide trust management capabilities to make trust decisions, which will greatly hinder the development of cloud computing. Fig.1 depicts the brokering scenario in existing brokers (e.g., RESERVOIR [18], PCMONS [19], RightScale [20], SpotCloud [21], and Aeolus [22]). We can see that this existing brokering archi-tecture for cloud computing do not consider user feedback only relying on some direct monitoring information.

As depicted in Fig. 2, C-provider architecture, a service brokering system is proposed based on direct monitoring information and indirect feedbacks for the multiple cloud environment, in which C-provider is designed as the TTP for cloud trust management and resource matching. Before introducing the principles for assessing, representing and computing trust, we first present the basic architecture of C-provider and a brief description of its internal components.

Figure-2



C-provider's Architecture and main function modules.kinds of trusted attributes of cloud services, which consists of node spec profile, average resource usage information, average response time, average task success ratio, and the number of malicious access. The node spec profile includes four trusted evidences: CPU frequency, memory size, hard disk capacity and network bandwidth. The average resource usage information consists of the current CPU utilization rate, current memory utilization rate, current hard disk utilization rate and current bandwidth utilization rate. The number of malicious access includes the number of illegal connections and the times of scanning sensitive ports.

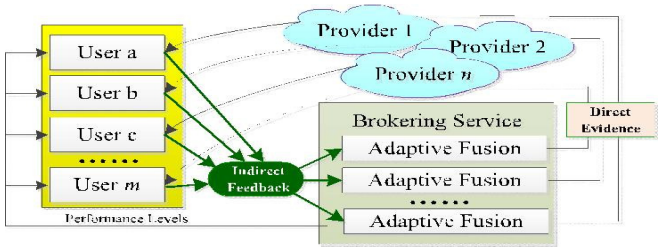
B. Virtual Infrastructure Manager (VIM)

Each cloud provider offers several VM configurations, often referred to as instance types. An instance type is defined in terms of hardware metrics such as CPU frequency, memory size, hard disk capacity, etc. In this work, the VIM com-ponent is based on the OpenNebula virtual infrastructure manager [42], [43], this module is used to collect and index all these resources information from multiple cloud providers. It obtains the information from each particular cloud provider and acts as a resource management interface for monitoring system. Cloud providers register their resource information through the VIM module to be able to act as sellers in a multi-cloud marketplace. This component is also responsible for the deployment of each VM in the selected cloud as specified by the VM template, as well as for the management of the VM life-cycle. The VIM caters for user interaction with the virtual infrastructure by making the respective IP addresses of the infrastructure components available to the user once it has deployed all VMs.

C. SLA Manager and Trusted Resource Matching

In the multiple cloud computing environment, SLA can offer an appropriate guarantee for the service of quality of resource providers, and it serves as the foundation for the expected level of service between the users and the providers [45], [46]. An SLA is a contract agreed between a user and a provider which defines a series of service quality characters. Adding trust mechanism into the SLA management,

Figure-3



C-provider' brokering scenario with adaptive fusion mechanism.

cloud brokering system can prepare the best trustworthiness resources for each service request in advance, and allocate the best resources to users. In general, the service resource register its services on the cloud brokering system. The service user negotiates with the service provider about the SLA details; they finally make a SLA contract. According to the SLA contract, the resource matching module selects.

D. Hybrid and Adaptive Trust Computation Model (HATCM)

Trust and feedback management systems are successfully used in numerous application scenarios to support users in identifying the reliable and trustworthy providers. Similar approaches are needed to support cloud brokering systems in matching appropriate trustworthy resources from different providers in a multi-cloud computing environment. HATCM module is not only the core of the trust-aware cloud computing system, but also a key task of this work. Using this module, the middleware architecture can sort high performance resources through analyzing the history information of the resources for providing highly trusted resources dynamically.

As depicted in Fig. 3, HATCM uses a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining real-time service behavior with the social feedback of the service resources. The HATCM allowscloud users to specify their requirements and opinions when accessing the trust score of cloud providers. That is, users can specify their own preferences, according to their business policy and requirements, to get a customized trust value of the cloud providers.

E. Services Feedback and Aggregation (SFA)

In large-scale distributed systems, such as grid computing, P2P computing, wireless sensor networks, and so on, feedback provides an efficient and effective way to build a social-evaluation-based trust relationship among network entities. By the same token, feedback also can provider important reference in evaluating cloud resource trustworthiness. Consider large-scale cloud collaborative computing environ-ment which host hundreds of machines and handles thousands of request per second, the delay induced by trust system can be one big problem. So, there is no doubt that the computational efficiency of a feedback aggregating mechanism is the most fundamental requirement. As depicted in Fig. 3, we build cloud social evaluation system using feedback technology among virtualized data centers and distributed cloud users, and we use a lightweight feedback mechanism, which can effectively reduce networking risk and improve system efficiency.

IV. CLOUD TRUST COMPUTATION MODEL

This section contains a lot of notations. At the beginning of this section, we list some key notations and their meanings in Table I to make it easier for the readers to follow up.Trustworthiness computation model and approaches are the core technologies of trust management. In our C-provider, we propose a hybrid and adaptive trust

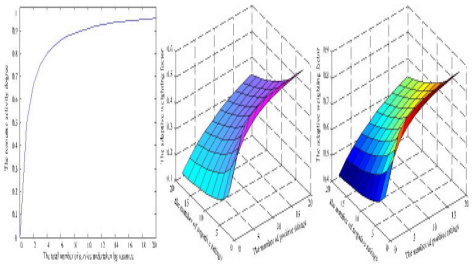
model to compute the overall trust degree of service resources, in which trust is a fusion evaluation result from adaptively combining real-time trust computation with the feedback of the service resources. In this section, we first present the adaptive real-time trust computation approach based on multiple key trust attributes of service resources. We then introduce the light-weight feedback trust computation approach. Finally, we discuss how to aggre-gate the two kind of trust factors with an adaptive mechanism.

A. Adaptive Real-Time Trust Computation

As mentioned in Part A of section III, to calculating resource trust degree from the perspective of QoS guarantee-ing, we mainly focus on five kinds of trusted attributes of cloud services [7], [10], [11], which consists of node spec profile, average resource usage information, average response time, average task success ratio and the number of malicious access. Both the node spec profile and average resource usage information include four trusted evidences.

Monitoring service behavior is the process of acquiring state information from a cloud resource. In traditional poll-based approach, monitoring is performed by a manage-ment node, which periodically polls nodes in its domain for the values of related parameters. An alternative to the poll-based approach, is the push approach, whereby network nodes send values of parameters to the manager whenever changes to those values occur. With the emergence of large and dynamic networked systems, the push approach is gaining importance, because this approach enables the management system to continuously follow the evolution of the network state [44]. In this work, we adopted the push-based approach to acquire these QoS indicators. We deployed two types of software sensors: (i) Monitoring sensors are responsible for collecting the direct performance indicators of computing resources. Such as CPU frequency, memory size, hard disk capacity, the number of illegal connections, the times of scan-ning sensitive ports etc. (ii) Computing sensors are responsible

Figure-4



IV. CONCLUSION AND FUTURE WORK

In this paper, we present C-provider, a trust-aware service brokering system for efficient matching multiple cloud services to satisfy various user requests. Experimental results show that C-provider yields very good results in many typical cases, and the proposed mechanism is robust to deal with various number of service resources. In the future, we will continue our research from two aspects. First is how to accurately calculate the trust value of resources with only few monitored evidences reports and how to motivate more users to submit their feedback to the trust measurement engine. Implement-ing and evaluating the proposed mechanism in a large-scale multiple cloud system, such as distributed data sharing and remote computing, is another important direction for future research.

REFERENCES

[1] M. Singhal*et al.*, "Collaboration in multicloud computing environments:Framework and security issues," *Computer*, vol. 46, no. 2, pp. 76–84,Feb. 2013.

[2] H. M. Fard, R. Prodan, and T. Fahringer, "A truthful dynamic workflowscheduling mechanism for commercial multicloud environments," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1203–1212, Jun. 2013.

[3] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy, and L. Seinturier,"A federated multi-cloud PaaSinfrastructure," in *Proc. 5th IEEE Int.Conf. Cloud Comput. (CLOUD)*, Jun. 2012, pp. 392–399.

[4] P. Jain, D. Rane, and S. Patidar, "A novel cloud bursting brokerageand aggregation (CBBA) algorithm for multi cloud environment," in*Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol. (ACCT)*, Jan. 2012,pp. 383–387.

[5] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing,"*IT Prof.*, vol. 12, no. 5, pp. 20–27, Sep./Oct. 2010.

[6] K. Hwang and D. Li, "Trusted cloud computing with secure resourcesand data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22,Sep./Oct. 2010.

[7] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model forQoS guarantee in cloud systems," *Int. J. Grid Distrib. Comput.*, vol. 3,no. 1, pp. 1–10, Mar. 2010.

[8] P. D. Manuel, S. ThamaraiSelvi, and M. I. A.-E. Barr, "Trustmanagement system for grid and cloud resources," in *Proc. 1st Int. Conf.Adv. Comput. (ICAC)*, Dec. 2009, pp. 176–181.

[9] L.-Q. Tian, C. Lin, and Y. Ni, "Evaluation of user behaviortrust in cloud computing," in *Proc. Int. Conf. Comput. Appl. Syst.Modeling (ICCASM)*, Oct. 2010, pp. V7-576–V7-572.

[10] X. Li and Y. Yang, "Trusted data acquisition mechanism for cloudresource scheduling based on

distributed agents," *Chin. Commun.*, vol. 8,no. 6, pp. 108–116, 2011.
[11] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust schemefor resource matchmaking across multiple clouds," *IEEE Trans. ParallelDistrib. Syst.*, to be published, doi: 10.1109/TPDS.2014.2321750.
[12] (2014). *OPTIMIS*.[Online]. Available: http://www.optimis-project.eu/
[13] W. Fan and H. Perros, "A novel trust management frameworkfor multi-cloud environments based on trust service providers,"*Knowl.-Based Syst.*, vol. 70, pp. 392–406, Nov. 2014.
[14] N. Ghosh, S. K. Ghosh, and S. K. Das, "SelCSP: A framework tofacilitate selection of cloud service providers," *IEEE Trans. Cloud*
Comput., vol. 3, no. 1, pp. 66–79, Jan./Mar. 2015.
[15] A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced securitymodel for trusted platform based services," *Future Generat.Comput.Syst.*, vol. 27, no. 5, pp. 564–573, 2011.
[16] S. M. Habib, V. Varadharajan, and M. Muhlhauser, "A trust-awareframework for evaluating security controls of service providers in cloudmarketplaces," in *Proc. 12th IEEE Int. Conf. Trust, Secur., PrivacyComput. Commun.*, Jul. 2013, pp. 459–468.
[17] T. H. Noor and Q. Z. Sheng, "Trust as a service: A framework fortrust management in cloud environments," in *Web Information System*
Engineering (Lecture Notes in Computer Science), vol. 6997. Berlin,Germany: Springer-Verlag, 2011, pp. 314–321.
[18] B. Rochwerger*et al.*, "The RESERVOIR model and architecture foropen federated cloud computing," *IBM J. Res. Develop.*, vol. 53, no. 4,
pp. 535–545, 2009.
[19] S. A. De Chaves, R. B. Uriarte, and C. B. Westphall, "Towardan architecture for monitoring private clouds," *IEEE Commun. Mag.*,vol. 49, no. 12, pp. 130–137, Dec. 2011.LI *et al.*: C-PROVIDER: A TRUST-AWARE SERVICE BROKERING SCHEME 1415
[20] (2014). *RightScale*.[Online]. Available: http://www.rightscale.com/
[21] (2014). *SpotCloud*.[Online]. Available: http://www.spotcloud.com/
[22] (2014). *Aeolus*. [Online]. Available: http://www.aeolusproject.org/index.html
[23] J. Spring, "Monitoring cloud computing by layer, part 1," *IEEE SecurityPrivacy*, vol. 9, no. 2, pp. 66–68, Mar./Apr. 2011.
[24] J. L. Lucas-Simarro, R. Moreno-Vozmediano, R. S. Montero, andI. M. Llorente, "Scheduling strategies for optimal service deploymentacross multiple clouds," *Future Generat. Comput. Syst.*, vol. 29, no. 6,pp. 1431–1441, Aug. 2013.
[25] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud security with virtualizeddefense and reputation-based trust management," in *Proc. 8th IEEEInt. Conf. Dependable, Autonomic, Secure Comput. (DASC)*, Dec. 2009,pp. 717–722.

AUTHORS PROFILE

]V.Savitha, Master of Engineering in Computer Science and Engineering from Anna University Coimbatore. She is currently working as Assistant Professor at SNS College of Technology, Coimbatore. Her research areas include Computer Network and Compiler Design .

B.Maheshkumar presently working as assistant professor in the Department of Computer Engineering at A.S.L Pauls College of Engineering and Technology Coimbatore. He received M.E in computer Engineering from Anna university Chennai.