Agent-Based Approach for the Management of Dynamic QoS Violations in the Inter-Cloud Environments

Manoj V. Thomas[1], K. Chandrasekaran[1(✉)], and Gopal Mugeraya[2]

[1] Department of Computer Science and Engineering, NITK, Surathkal, India
manojkurissinkal@gmail.com, kchnitk@ieee.org
[2] NIT Goa, Farmagudi, India
director@nitgoa.ac.in

Abstract. Nowadays, considerable attention has been given by the researchers in the field of Cloud Computing to the emerging Inter-Cloud computing paradigm, where different cloud service providers collaborate or federate to achieve better QoS and cost efficiency. In this context, in order to prevent the unauthorized access of the distributed system components, authentication and authorization functions are to be enforced effectively. In this paper, we propose the conceptual model of the agent-based approach for the identity and access management in the dynamic inter-cloud environments where the Cloud Service Providers or the partners of the inter-cloud federation join and leave the federation dynamically. We further discuss the architectural model for the agent-based approach for solving the policy conflicts in the inter-cloud scenario while dealing with the access requests of cloud consumers in the inter-cloud environments. A few open issues in the area of identity and access management in the inter-cloud environment are also discussed.

Keywords: Access control · Agents · Authentication · Authorization
Inter-cloud · Policy-conflict · Trust

1 Introduction

1.1 Inter-Cloud Scenario

In the inter-cloud or cloud federation environment, different cloud service providers (CSPs) collaborate to provide better services to the cloud users, and thereby increasing their resource utilization and business prospects. The CSPs will have service level agreements between them for the resources and services offered to other CSPs in the inter-cloud environment [1].

L. Uden et al. (Eds.): KMO 2018, CCIS 877, pp. 477–488, 2018.
https://doi.org/10.1007/978-3-319-95204-8_40

1.2 Need for the Management of Dynamic QoS Violations in the Cloud Federation

Generally, there will be Service Level Agreements (SLAs) between the partners in the inter-cloud or federation to share the resources. Due to the dynamic nature of customer requirements, sometimes a CSP in a federation may urgently need some resources from other CSPs in the federation to meet the customer requirements, as the requested resources are unavailable with the CSP at that time. Since the CSPs in the inter-cloud environment operate by the Service Level Agreements among them, a CSP can get the services as per the QoS agreement in the SLA. Normally, the process of SLA renegotiation is carried out among the CSPs in order to modify the QoS parameters of the services agreed among them. Now, if a request comes to a CSP from another CSP in the federation for some resources whose QoS features are not as per their prior agreement, how to deal with such a request in the federation dynamically without the time consuming SLA renegotiation at that time is an issue to be considered. QoS/SLA violation in the inter-cloud occurs when one CSP requires some service from another CSP whose QoS features differ from what have been agreed in the SLA between them.

1.3 Agent-Based Computing

Agents are normally autonomous programs, which can interact with the environment and act upon it to achieve their tasks [2]. A multi-agent system involves multiple interacting software components known as agents, which can cooperatively solve the problems that are beyond the capabilities of any individual entity.

The rest of the paper is organized as follows: Sect. 2 describes the work done in the area of identity and access management in the inter-cloud environments, highlighting the merits and demerits of various approaches. Section 3 presents the agent-based approach for identity and access management in the dynamic inter-cloud environments. Section 4 discusses the agent-based model for dealing with the dynamic policy conflicts management in the inter-cloud scenario. Section 5 shows the analysis and results mentioning a few open issues in this area and Sect. 6 concludes the paper.

2 Literature Review

The research in the field of Identity and Access Management in the Inter-Cloud environment is still in its nascent stage, and some of the relevant approaches proposed by the researchers in that area is given in this section. In [3], the authors propose the architecture for Federated Identity Management in a scenario similar to the Inter-Cloud environment. The work focuses on sharing of information or resources across all the three cloud service models such as SaaS, PaaS and IaaS. The works carried out in [4–7] present a heterogeneous horizontal cloud federation model, for CLoud-Enabled Virtual EnviRonment (CLEVER). These works

use the concept of a middleware component called the Cross-Cloud Federation Manager (CCFM) that could be integrated into the Cloud Manager component of the Cloud Service Provider. This work does not discuss the issue of policy conflict management in the inter-cloud scenario.

The authors presented a blueprint for the design of Inter-cloud in [8–10]. This blueprint is designed considering the Interoperability factor between the various Cloud Service Providers and is focused at the Internet scale. The work in [11] discusses the inter-cloud security considerations. In [12], the authors propose an authentication mechanism for inter-cloud environments using SAML profile over XMPP. The architecture discussed in this work is based on the internet scale. The issue of policy conflict management and the break-glass mechanism is not clear in these architectures. In the work carried out in [13], the Cloudbus toolkit is discussed which includes the various Cloud solutions, technologies and components to build a global Cloud computing marketplace. In the work presented in [14], the authors propose an architecture for the Inter-cloud scenario, which is based on the market-oriented Cloud Computing, an essential part of the Cloudbus toolkit. This architecture requires the Aneka Container to be installed at all the required cloud nodes.

The work shown in [15] discusses a Federated Identity Management approach using Hierarchical Identity-Based Cryptography. The work focuses on the Private Key Generator (PKG) hierarchical model. This model assumes a root PKG for managing the entire Hybrid Cloud. The root PKG generates private keys for PKGs of the member Clouds associated with the hybrid cloud. In this work, the Federated Identity Management functionalities are distributed between root PKG and individual cloud level PKGs [16]. Before applying this model to the inter-cloud scenario, issues regarding the control of the root PKG should be solved. The authors carry out an analysis of the cost benefits of resource sharing in cloud federation in the work presented in [17]. The Cloud Scheduler project explained in [18], focuses on developing a model for resource provisioning and sharing among the various participating Clouds. In this work, the authors concentrate more on the scheduling of applications among the partners in the federation, and not on establishing the federation.

Based on the literature review, it is seen that the proper solution for the issue of IAM in the inter-cloud computing needs extensive research in the area of trust establishment and conflict management of access policies for accessing various resources.

3 Agent-Based Identity and Access Management (IAM) in the Dynamic Inter-Cloud Environments

In this section, we are proposing an agent-based architecture for the IAM in the inter-cloud environment, when the CSPs or the partners join or leave the federation dynamically. Inter-cloud environment is formed with the aim of improving the QoS that could be delivered to the cloud customers. It is an association between different CSPs in order to achieve better QoS and the economy of scale.

But, in this cloud environment, practically, we cannot expect the inter-cloud environment to be static. That means, for example, if we start a federated cloud environment at a time t_1 with n CSPs, where $n > 0$, we cannot expect that inter-cloud environment to remain the same over time, since the CSP's ultimate aim is to increase their revenues by delivering quality services and thereby attracting more customer base. Hence, at any other point of time t_2, the number of partners in that federated cloud environment may change to m, where m could be either greater or less than or equal to n. Also, even if the number of partners remain the same as n, the current partners could be different from those present before.

3.1 Conceptual Model

The proposed high level conceptual model is shown in the Fig. 1. The major elements or actors in our proposed model are Cloud Service Consumer (CSC), Cloud Service Provider (CSP), Access Request Mediating Agent (ARMA) and the Identity Provider (IdP). The proposed high level conceptual model is shown in the Fig. 1.

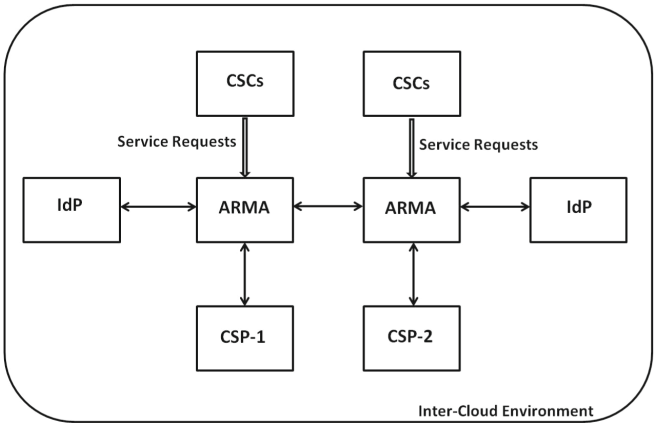

Fig. 1. Agent-based approach for identity and access management in the dynamic inter-cloud

3.2 Components of the Proposed Model

The major functional components identified in the model are:

Cloud Service Consumer (CSC). Cloud Service Consumers are the entities requesting the resources or services from the Cloud Service Providers (CSPs) in the inter-cloud environment. The CSCs need to be properly authenticated and their access rights need to be verified in order to ensure that unauthorized users do not access the services hosted by the CSPs.

Access Request Mediating Agent (ARMA). This agent runs on every Cloud Service Provider which is acting as a partner in the inter-cloud environment. The ARMAs of various partners in the inter-cloud interact with each other as shown in the Fig. 1, where only two CSPs of the cloud federation namely CSP_1 and CSP_2 are shown. The individual users of a CSP in an inter-cloud interact with the ARMA of the respective CSP, which further interact with the underlying cloud layer for resource provisioning.

Cloud Service Provider (CSP). In the inter-cloud, the CSPs have an agreement between them to share their virtualization infrastructure and resources with other CSPs in order to meet the objectives of the cloud federation, and they offer various services such as IaaS, PaaS or SaaS to the various users requesting services in the inter-cloud environment.

Identity Provider (IdP). IdPs are third parties trusted by the CSPs in the inter-cloud environment for providing the identity management of the cloud users. The IdP implements the federated identity management in the inter-cloud enforcing Single Sign-On (SSO).

The ARMA of a CSP perform the various identified tasks or functions involved in the effective dynamic inter-cloud management. The various functional components of the ARMA, and their interactions are shown in the Fig. 2. The required components are:

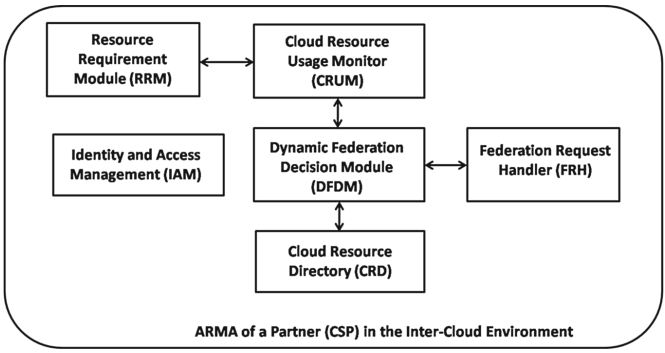

Fig. 2. Access Request Mediating Agent (ARMA) in the dynamic inter-cloud

A. Resource Requirement Module (RRM)
This module of the ARMA identifies the current resource requirements made by the cloud customers at any point of time. It also interacts with the Cloud Resource Usage Monitor Module to know the present utilization level of the cloud resources hosted by that particular CSP. In case the RRM module finds that the resources are already saturated, the module publishes the resource requirement

details in the inter-cloud environment so that the information is available to other clouds who are either members of the federation, or who would like to form the federation with the existing inter-cloud. The information should be published using technology or protocol such as eXtensible Messaging and Presence Protocol (XMPP) or Advance Message Queuing Protocol (AMQP) so that the partner clouds can meet the purposes of federation formation.

B. Cloud Resource Usage Monitor (CRUM)
This module helps to identify the resource usage details of the parent cloud where the resource requests are originated by the cloud customers. Also, the resource usage details of other clouds who are partners of the federation could be monitored by this module by interacting with the Cloud Resource Directory (CRD) maintained at the respective CSP in the inter-cloud.

C. Federation Request Handler (FRH)
When a CSP receives a request, this module takes the decision of forming the federation with that requesting CSP. The important components involved in this module are:

(i) Trust Evaluation (TE). The trust value of a CSP could be based on the past behavior and the history of previous transactions with the same CSP. There could be a trust model which should be implemented, and the trust threshold value could be set in the inter-cloud environment. **(ii) Policy Matching (PM).** Before taking a final decision on the request of any CSP to form the federation, the policies of that CSP should match with that of the federation. The various aspects of the policies could include the type of the resources and the services offered, the authentication and the authorization mechanisms adopted by the CSP, the QoS guaranteed by the CSP and also the type of the SLA it makes.

D. Dynamic Federation Decision Module (DFDM)
This module adopts a threshold-based permission scheme to deal with the dynamic inter-cloud formation. The feedback of FRH is communicated to this DFDM module and the DFDM broadcasts the join-request to all the existing partners in the inter-cloud. If k out of n existing partners, where k is the threshold agreed by all the n existing partners in the inter-cloud, permit the new cloud to be a part of the federation, the DFDM module registers the new cloud. In our proposed model, the DFDM of the cloud where a CSP makes the request to be a part of the existing federation, coordinates this activity of accepting the new CSP as a partner. Again, the decision to terminate a federation relationship has to be achieved among all the existing inter-cloud partners and Dynamic Federation Decision module coordinates this activity.

E. Cloud Resource Directory (CRD)
Once the cloud federation is formed, this module of a partner CSP stores the details of the various services offered by other partners in the federation, so that a CSP can identify any other CSP in the inter-cloud that offer similar services as requested by the cloud customers. Whenever there is a new CSP being added to the inter-cloud, or any CSP being removed from the existing federation, this CRD needs to be updated.

F. Identity and Access Management Module (IAM)
Whenever an access request is received by a CSP in the inter-cloud, this module of the ARMA deals with the authentication and authorization processes of the cloud customers. This component of the IAM module involves verifying the identity of the requesting user by interacting with the Identity Provider using SAML assertions. Events of possible policy conflicts, arising out of the various access requests made by different users which need to be satisfied by more than one CSP at a time in the cloud-federation are handled by this module of the ARMA.

4 Dynamic Policy Conflicts Management in the Inter-Cloud Environments

Whenever a service request from a cloud user is processed by a CSP, the applicable policies are considered for determining the access rights of the cloud users specific to a CSP. The major policies of the CSPs like the details of the resources or services offered, the QoS delivered, list of Identity Providers supported, SLAs, the authentication and the authorization mechanisms supported by the CSP etc. are considered while forming the federation with any CSP. In the inter-cloud environment, a CSP who is unable to satisfy the request of a cloud customer might offload the service requests to the partners in the federation who offer the similar services. Suppose that there is an SLA agreed between CSP-A and CSP-B in the inter-cloud. Also, assume that as per the SLA, CSP-B has agreed to give the service consisting of a maximum of n number of VMs of type 'small' to CSP-A. Now, imagine that CSP-A makes a service request of m VMs ($m > n$). Also the type of the VMs requested is 'large'. This is an example of the QoS/SLA violations between the CSPs. Hence, in order to make the best use of the federation, we need a dynamic management of this possible QoS violations among the partners in the federation so that the mutual benefits of the CSPs in the federation, in terms of reliability, reputation and the economic benefits are improved.

In this section, we propose an agent-based mechanism to solve such a scenario of policy conflicts in the inter-cloud environment. With reference to the Fig. 1 in Sect. 3, the proposed conceptual architecture of the ARMA for dynamic policy conflicts management is shown in the Fig. 3. The various functional components in the architecture are:

4.1 The Resource Request Handler (RRH)

This module of the ARMA deals with the service requests initiated by the cloud customers requesting various services from the inter-cloud. The module interacts with the Context Handler (CH) module, and identifies the type of request made by the cloud customers such as the service requested, requested resource details, and various other parameters such as the QoS, duration of the service required, SLA details etc.

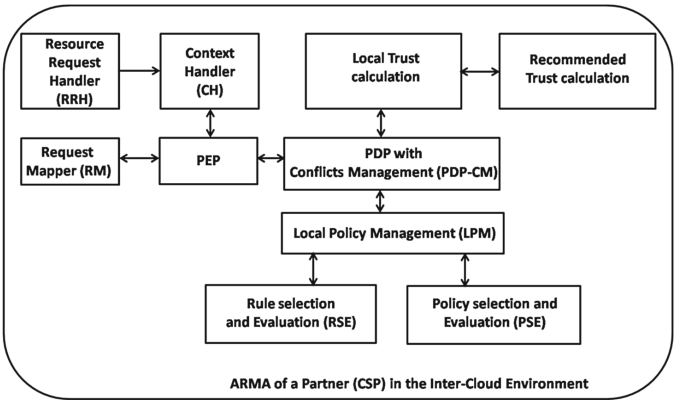

Fig. 3. Access Request Mediating Agent (ARMA) with policy conflicts management in the dynamic inter-cloud

4.2 Context Handler (CH)

This module of the ARMA is required to convert the service requests from the format submitted by the cloud users to a specific format (such as XACML format) which could be used for further processing using access control languages such as XACML, in the inter-cloud environment.

4.3 Policy Enforcement Point (PEP)

This module implements the access control decisions taken by the Policy Decision Point (PDP) module. When the resource request comes to the CSP form a cloud customer, the Context Handler Module converts the request to the common policy format, and the PEP responds to the access requests based on the access control decision of the PDP. The PDP module contacts the Local Policy Management Module.

4.4 Local Policy Management Module (LPM)

This module considers the applicable policies and their evaluation related to any particular access request initiated by the clients. Thus, this module takes the authorization decision of permitting or denying the access request initiated by the cloud customers based on the rules and the policies evaluation. This module updates the PDP with the decision obtained after selecting and evaluating the various applicable rules and policies with respect to the access request received.

4.5 PDP with the Conflicts Management (PDP-CM)

In the inter-cloud environment, if the decision of the Local Policy Management Module is to deny the access request initiated by a CSP, this module comes into

action. In order to solve such an issue, in the proposed architectural solution, the PDP is implemented with the Conflicts Management in such a way that it calculates the direct and recommended trust values of the CSP in the inter-cloud environment, and based on the trust value of the requesting CSP, it takes a decision as to accept or reject the access request from other partners in the federation.

4.6 Local Trust Calculation

This module of the ARMA calculates the local trust values of the requesting CSP. This calculation is based on its own experience of working with the requesting CSP in the past. This calculation takes into account various parameters such as how many successful interaction they had between them in the past, and how long the requesting CSP has been a part of the inter-cloud or federation environment etc. If the calculated trust value is greater than the trust threshold maintained buy the CSP, the access request is accepted even if there is a QoS violation between the CSPs in the federation.

4.7 Recommended Trust Calculation

If the trust values calculated by the Local Trust Calculation module is less than the trust threshold, recommended trust of the requesting CSP is calculated. This calculation involves identifying the trusted CSPs in the inter-cloud environment, and then taking feedback of the requesting CSPs from the trusted CSPs. The final trust value can be calculated as the average of the local and the recommended trust values of the requesting CSP. If the final trust value is greater than the trust threshold, the access request is accepted, otherwise rejected.

4.8 Request Mapper

There is a need to map the resource requests initiated by the various cloud users in the inter-cloud to the corresponding format or APIs supported by their respective Cloud Service Providers to get the service done. Hence, after verifying the access privileges of the inter-cloud customers, the Request Mapper module maps the requests of cloud customers to their underlying infrastructure-specific interfaces.

5 Analysis and Results

5.1 Experimental Setup

We have carried out the simulation experiments on a system with Intel (R) Core (TM) i7-3770, CPU 3.40 GHz, 8.00 GB RAM and 32-bit Operating System (Ubuntu 14.04). Softwares used for the implementation include CloudSim-3.0.3, Eclipse IDE version 3.8, MySQL Workbench Community (GPL) for Linux/Unix version 6.0.8 and Java version 1.7.0_55.

5.2 Results

In order to test and validate the proposed approach in the Cloud Federation environment, we have implemented the Cloud Federation of 25 CSPs using the CloudSim toolkit [19]. The Fig. 4 shows the behavior of the proposed Agent-Based Dynamic QoS Management Mechanism. In the figure, the X-axis shows the three cases in solving the QoS violations. In the proposed approach, whenever there is a violation, trust value of the requesting CSP is calculated by the ARMA. Here, case 1 shows the number of requests accepted using the local trust of the CSP. Case-2 shows the number of resource requests accepted by calculating the local and the recommended trust of the requesting CSP. Case 3 shows the number of cases in which calculated trust value was not sufficient to accept the resource request from the CSP in the inter-cloud. (Out of 80 access requests made by CSP-1, 24 times requests were accepted using the local trust of the CSP and 38 times resource requests were accepted by calculating the local and the recommended trust of the requesting CSP. Also, 18 times the calculated trust value of CSP-1 was not sufficient to accept the resource request from the CSP in the inter-cloud. This approach can be extended to analyze the performance of other CSPs in the inter-cloud as well.

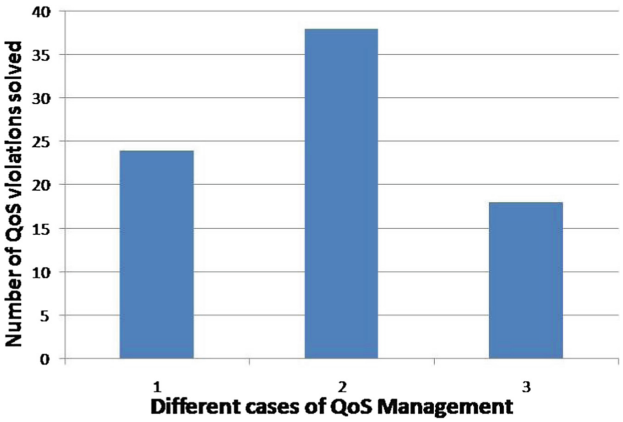

Fig. 4. Graph showing the behavior of the proposed dynamic policy-conflicts management mechanism

Based on the analysis done, it is seen that effective management of the QoS violations is required to improve the efficiency or throughput of the inter-cloud environment. It is also seen that most of the research works do not provide effective solutions, as far as implementing an effective policy conflicts management in the inter-cloud environment. The Inter-Cloud paradigm is considered as the future of cloud computing, and the agent-based identity and access management mechanism has enormous potential for further active research, in order to make the inter-cloud computing paradigm secure, reliable and scalable.

6 Conclusion and Future Work

This paper discusses an approach for the agent-based identity and access management in the dynamic inter-cloud environment with policy conflicts management considering the requirements of the current inter-cloud scenario. We have also analyzed the existing identity and access management approaches, mentioning their pros and cons in the inter-cloud environment. It is seen that, the research activities in the area of identity and access management in the inter-cloud is still in the nascent stage and the effective management of policy-conflicts in the inter-cloud environment is needed for the effective use of the paradigm. A few open issues for further research in the areas of identity and access management are also discussed. As a future work, we plan to simulate and study in detail, the mechanisms for the dynamic inter-cloud management and the dynamic policy-conflicts management mechanisms.

References

1. Global inter-cloud technology forum, use cases and functional requirements for inter-cloud computing. Technical report (2010)
2. Wooldridge, M.: An Introduction to Multiagent Systems. Wiley, Hoboken (2002)
3. Stihler, M., Santin, A.O., Marcon, A.L., da Silva Fraga, J.: Integral federated identity management for cloud computing. In: Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5 (2012)
4. Celesti, A., Tusa, F., Villari, M., Puliafito, A.: How to enhance cloud architectures to enable cross-federation. In: Proceedings of the 3rd International Conference on Cloud Computing (CLOUD), pp. 337–345 (2010)
5. Celesti, A., Tusa, F., Villari, M., Puliafito, A.: Security and cloud computing: intercloud identity management infrastructure. In: Proceedings of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), pp. 263–265 (2010)
6. Celesti, A., Tusa, F., Villari, M., Puliafito, A.: Three-phase cross-cloud federation model: the cloud SSO authentication. In: Proceedings of the Second International Conference on Advances in Future Internet (AFIN), pp. 94–101 (2010)
7. Tusa, F., Celesti, A., Paone, M., Villari, M., Puliafito, A.: How CLEVER-based clouds conceive horizontal and vertical federations. In: Proceedings of the IEEE Symposium on Computers and Communications (ISCC), pp. 167–172 (2011)
8. Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., Morrow, M.: Blueprint for the intercloud - protocols and formats for cloud computing interoperability. In: Proceedings of the Fourth International Conference on Internet and Web Applications and Services, ICIW 2009, pp. 328–336 (2009)
9. Bernstein, D., Vij, D., Diamond, S.: An intercloud cloud computing economy-technology, governance, and market blueprints. In: Proceedings of the SRII Global Conference (SRII), pp. 293–299 (2011)
10. Bernstein, D., Vij, D.: Intercloud exchanges and roots topology and trust blueprint. In: Proceedings of the 2011 World Congress in Computer Science, Computer Engineering and Applied Computing (2010)
11. Bernstein, D., Vij, D.: Intercloud security considerations. In: Proceedings of the Second IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 537–544 (2010)

12. Bernstein, D., Vij, D.: Intercloud directory and exchange protocol detail using XMPP and RDF. In: Proceedings of the 6th IEEE World Congress on Services (SERVICES-1), pp. 431–438 (2010)
13. Buyya, R., Pandey, S., Vecchiola, C.: Cloudbus toolkit for market-oriented cloud computing. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 24–44. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_4
14. Buyya, R., Ranjan, R., Calheiros, R.N.: InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In: Hsu, C.-H., Yang, L.T., Park, J.H., Yeo, S.-S. (eds.) ICA3PP 2010. LNCS, vol. 6081, pp. 13–31. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13119-6_2
15. Yan, L., Rong, C., Zhao, G.: Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 167–177. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_15
16. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_34
17. Goiri, I., Guitart, J., Torres, J.: Characterizing cloud federation for enhancing providers' profit. In: Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD), pp. 123–130 (2010)
18. Armstrong, P., Agarwal, A., Bishop, A., Charbonneau, A., Desmarais, R., Fransham, K., Hill, N., Gable, I., Gaudet, S., Goliath, S., Impey, R., Leavett-Brown, C., Ouellete, J., Paterson, M., Pritchet, C., Penfold-Brown, D., Podaima, W., Schade, D., Sobie, J.: Cloud scheduler: a resource manager for distributed compute clouds. CoRR, abs/1007.0050 (2010)
19. Calheiros, R.N., Ranjan, R., Beloglazov, A., De Rose, C.A., Buyya, R.: CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Softw. Pract. Exp. **41**(1), 23–50 (2011)