A MAS-Based Cloud Service Brokering System to Respond Security Needs of Cloud Customers

Jamal TALBI[1], Abdelkrim HAQIQ[1,2]

[1]Computer, Networks, Mobility and Modeling laboratory, Department of Mathematics and Computer, Faculty of Sciences and Techniques, Hassan 1st University, Settat, Morocco,
[2]e-NGN Research group, Africa and Middle East

***Abstract* — Cloud computing is becoming a key factor in computer science and an important technology for many organizations to deliver different types of services. The companies which provide services to customers are called as cloud service providers. The cloud users (CUs) increase and require secure, reliable and trustworthy cloud service providers (CSPs) from the market. So, it's a challenge for a new customer to choose the highly secure provider. This paper presents a cloud service brokering system in order to analyze and rank the secured cloud service provider among the available providers list. This model uses an autonomous and flexible agent in multi-agent system (MASs) that have an intelligent behavior and suitable tools for helping the brokering system to assess the security risks for the group of cloud providers which make decision of the more secured provider and justify the business needs of users in terms of security and reliability.**

***Keywords* — Cloud Computing, Brokering System, Multi-agent System, Security Risk.**

I. Introduction

Cloud computing [1] is a new paradigm of utility computing and enormously growing phenomenon in the present IT industry hype .Many companies, enterprises and organizations outsource some of their information systems to benefit from the cloud services which are Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). The main interesting features of a cloud are the cost decrease and a faster time to market. Based on sharing resources, the cloud computing changes the user concerns from managing an infrastructure to only focusing on their core business. Currently there are many numbers of providers, but finding the best cloud service provider is difficult. Thus, it is a challenge for the users to choose the more secured cloud provider for fulfilling their requirements.

Nowadays, a few efforts have been devoted to building tools and frameworks that can permit customers to evaluate cloud offerings and rank them based on their ability to meet the user's quality of service (QoS) and security requirements. This is a major problem for every user, especially those who are more concerned about data security and privacy from CSP. For this purpose, cloud brokers [2] have emerged; they can help cloud consumers to select adequate solutions by comparing existing offers, essentially against their prices.

A secure computer system provides guarantees regarding the confidentiality, integrity, availability, non-repudiation and authenticity of its objects (such as data, processes or services). Security is related to vulnerabilities in software, and these are hard to foresee or detect before an actual attack; security involves personal aspects (e.g., user or operator issues) and aspects of the operational environment that are often beyond the control of the development teams. As cloud computing presents new kinds of security risks [3], [4], they need to be treated before wider adoption. Accordingly, we have to dispose a system that measure and rank the secured cloud service providers and then, the cloud services can make a major impact and will craft a healthy competition among cloud providers to satisfy their service level agreement (SLA) and improve their QoS and trustworthiness.

In this paper, our aim is to help a new customer to find the most reliable and secured CP in terms of security and trust through a brokering system integrating multi-agent systems that consists of user agents, providers agents, and broker agents, based on the principle that agent flexibility, intelligence, pro-activity, and autonomy can help cloud computing platforms offer solutions, functionalities, and intelligent services that can define, analyze, measure and rank the cloud service providers using a security risk analysis. Thus, the obtained results make decision of the best option of CP and justify the business needs in terms of security and reliability.

Multi-agent systems [5] represent a distributed computing paradigm based on multiple interacting agents that are capable of intelligent behavior. MASs can often solve problems using a decentralized approach in which several agents cooperate to generate efficient solutions. On the basis of collective AI approaches, developers can embed intelligence within software agents and deploy them on parallel or distributed computers to achieve the high performance required for solving large complex problems while keeping execution time low.

In this context, MASs should include self-detection of failures and self-monitoring of cloud operations and services, QoS security negotiation and SLA management, service-level agreement negotiation [6] [7], cloud interoperability, cloud resource brokering, virtual machines and service migration policies, dynamic scheduling. They're designed to operate in a dynamically changing environment.

The rest of the paper is organized as follows. The next section discusses related work. Section 3 describes the cloud service brokering system. The connection procedure of user and provider agents is presented in Section 4. In Section 5, an implementation and the experiment results in a case study are presented. Finally, Section 6 concludes the paper.

II. Related work

Security metrics are one of criteria that play a major role in ranking service providers. A cloud user may require an efficient, cost effective and basically more secured provider for his application. Since there are many providers who will provide same type of services with different level of security, so it will be a challenge for the user to select. Our motivation in this paper is to promote a novel approach for selecting the secured providers based on measuring security risks of cloud services.

In the same context, many researchers have proposed different approaches to help customer in this mission to select the appropriate cloud service. A collaborative filtering approach [8] rank the items based on similar user's preferences. This algorithm aggregates all the

DOI: 10.9781/ijimai.2017.4310

items purchased by the users and eliminate those items and ask users to rate the remaining services. In [9], cloud rank approach proposed greedy algorithm. It gives a method to rank cloud providers based on existing customer's feedback. It ranks component rather than service of providers. But there is no guarantee that all explicitly rated items by customers are ranked properly. But similar users will experience the same with same cloud providers so for them this approach will be helpful.

QoS-aware web by collaborative filtering [10] proposed a collaborative approach to rank providers on the basis of its web services. This method is useful for the customers who want to get an appropriate cloud provider which provides suitable web services. Thus, this method includes experience of users who used the services already and a hybrid collaborative filtering approach for evaluating web service QoS parameters.

Parveen Dhillon [11] proposed an effective and efficient method to select best cloud service. In order to select the best provider, three parameters are considered. Instead of taking all three parameters together applied. They made a ranking in where the best provider obtained is selected.

Zibin Zheng [12] proposed an approach for ranking equivalent cloud service providers by providing the similar kind of services which will help users to select suitable providers without spending much time for it. This method uses some QoS parameters for predicting best provider.

Deepak Kapgate [13] proposed a predictive broker algorithm based on Weighted Moving Average Forecasting Model (WMAFM). It proposes a new method to balance load on data centers and also minimizes response time. So for end users, they can get their requested service within few seconds.

Subha [14] had done a survey on quality of service ranking cloud computing. Here the author considered few qualities of service parameters and ranked providers based on that.

Cloud Rank [15] approach measures and ranks cloud services for the users. It takes the feedback or rating of users who had used the services already.

An efficient approach [16] find the best cloud provider by using a system for ranking cloud services based on QoS parameters such as service response time, cost, interoperability and suitability. It uses a broker algorithm that classify the existing providers and find out the more effective and efficient provider.

A sophisticated study [17] proposed ranking frameworks in cloud computing based on QoS parameters to select the best possible service provider.

Gani [1] proposed a conceptual model of federated third party cloud ranking and monitoring system (CMFCSPRS) that assures and boosts up the confidence to make a feasible secure and trustworthy market of CSPs.

III. The Conceptual Model of Cloud Service Brokering System (CMCSBS)

We consider the following scenario for explaining our approach. Let a scenario of a new cloud customer; say a company owner or manager is considering adopting cloud facility for the company. Main priority and mandatory condition is to protect company data security and privacy. The manager can see lots of cloud service provider in the market but not adequate guidelines to adopt the best secured cloud service provider for an organization. New cloud customer needs the security and trust certificate or report of these providers for making a decision to choose the right provider in terms of reliability, security and trustworthiness. So, clearly security issues are the most significant issue which is impeding the growth of mobile cloud computing [18] [19]. However, few ranked systems are available in service provisioning or performance issues but not adequate cloud service provider security ranking system is currently available.

In front of the several security issues [20] [21], we need to have some sort of monitoring, assurance and trust which not only come from the cloud service provider but also from a trusted cloud brokering system as shown in Fig. 1.

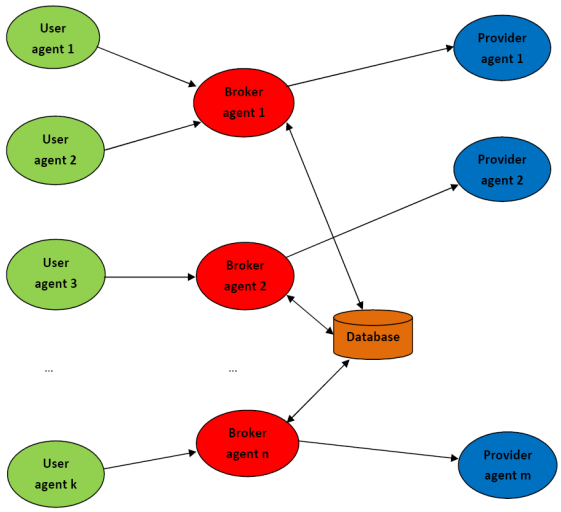

Fig. 1. Overview of the conceptual model of the cloud service brokering system (CMCSBS)

Our cloud service brokering system [22] consists of multiple broker agents, user agents, provider agents, applications and resources. Thus, the proposed model can be described into four-stage in terms of its architecture. First, the user agents send the requests to a broker agent. Second, the broker agent checks whether advertisement and request queues are empty. In case these queues are not empty, the broker agent carries out connection procedures (security needs, risk evaluation and recommendation). In case these queues are overloaded, the broker agent sends those requests (respectively, the advertisements) to other broker agents for balancing the workloads. Third, after executing the connection procedure, the broker agent sends the result to both user and provider agents. Fourth, if a user agent fails to connect to a provider agent, the broker agent recommends another broker agent that has the most potential in the brokering system via the database so that the user agent can send a request to another broker agent. Thereby, the three kinds of agents can be described based on their functionalities as follows.

A. User Agent

User agents provide user interface to the users of the system. They post requests to broker agents using message passing. If the connection procedure is completed, they show the results to user through a user interface.

B. Provider Agent

Provider agents have similar functionalities as user agents but act on behalf of human providers.

C. Broker Agent

The broker agent connects user and provider agents together using the connection algorithm. The broker agent can send a recommendation message based on the historical data of other broker agents in database, so that the broker agent can recommend other broker agents to the user agents which failed to connect to provider agents.

In the summary, the proposed system can act as a middleware between customer and cloud service provider and develops a model to find out the secured cloud service providers based on a connection procedure between the user and provider that will be presented in the next section.

IV. Description of the Connection Procedure of the CSBS

Probably all cloud service providers have a Service Level Agreements (SLA), but most of these SLAs were written to protect the vendors as opposed to being customer-centric. That has to change, and customers have to demand more with regard to service and the assurance of it. In the same time, cloud providers should protect their data or services from risk and harm. For this aim, the CSBS will conduct vulnerability and threat scans of components and services of the existing providers. The obtained results were fed into the risk evaluation that offer a list ranked of the secured providers.

The connection procedure (security needs, risk evaluation, and recommendation) between users and providers for selecting secured CSPs is presented as shown in Fig. 2. In this context, some assumptions and conditions should be considered as follows [1]:

- The CSBS must maintain the trust and reliability.
- The CSBS has enough resources to provide for processing and executing their own work.
- The system must be maintained and regulated by strict laws and transparent policies.
- Both the CSBS and CSPs mutually agree before executing the software penetration test.
- We consider that a CSP provide IaaS, PaaS and SaaS of its own.
- The CSBS is only the responsible of computing security metrics from sources and processes these measures for ranking results.
- A new cloud user looking for security and reliability should pay to the CSBS to see the ranked results.

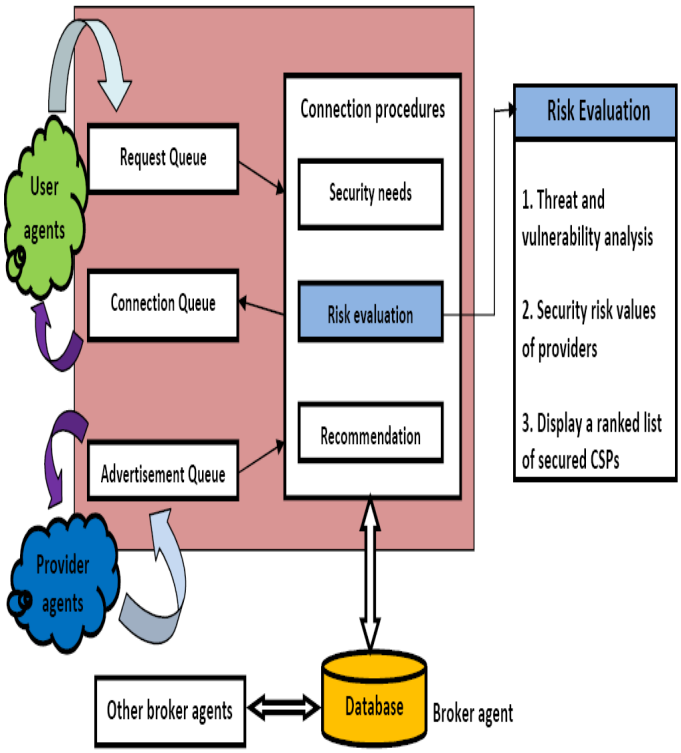

Fig. 2. The architecture of the CSBS

A. Security Needs Stage

The broker collects security requirements from user. It may be infrastructure requirements, platform requirements or software requirements. It uses the five CIANA objectives (Confidentiality, Integrity, Availability, Non-Repudiation, and Authenticity) to define the security need of each cloud user. If the customer needs the objective, the value is equal to 1, otherwise to 0.

B. Risk Evaluation Stage

All the registered cloud service providers give all the services which they are providing. Cloud broker contains the level of security of cloud providers. So the client gives requirements to broker, it checks the provider's performance based on criteria that are risks computed.

1) Threat and Vulnerability Analysis:

A vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm [23]. The identification of these vulnerabilities has been used by several approaches and researchers to estimate risks of the systems. In our case, we take into account five cloud security threats given by the Cloud Security Alliance (CSA) [24] to evaluate the risks. These threats are each related to the 5 CIANA objectives:

- Data Breaches = {Confidentiality}
- Data Loss = {Availability, Non-Repudiation}
- Account Hijacking = {Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity}
- Insecure Interfaces = {Confidentiality, Integrity, Authenticity}
- Denial of Service = {Availability}

We combine these relations with the security needs of each cloud user to obtain a function called harm. This later is defined on each customer, for each threat through the sum of the affected security needs. For example, the Insecure Interfaces threat (t) has the following harm on the cloud user (k) with the security needs (Confidentiality, Integrity, Non-Repudiation):

$$Harm\ (t, k) = (1 \times 1) + (1 \times 1) + (0 \times 0) + (0 \times 1) + (1 \times 0) = 2 \quad (1)$$

where the first value of each bracket is equal to 1 if the threat corresponds to the objective, 0 otherwise, and the second value is related to the security need.

2) Measuring Security Risk Assessment:

Once we calculate the harm of the threats on each cloud user, we have to determine the response to these threats for each cloud provider. For this aim, we use the STAR Registry and the matrix defined by the CSA [24].

The CSA matrix defines a list of security controls that a cloud provider should implement to reduce security risks. Each of these controls can be related to one or multiple threats. In addition, the STAR Registry publishes the list of implemented controls for providers willing to follow these recommendations.

In our case, we use these two information as binary values (a control mitigates a threat or not / a control is implemented by a provider or not) to calculate the coverage score, which indicates the response of a provider to a given threat. This value is a percentage, if the provider implements all controls mitigating a threat, it gets a coverage for this threat of 100%. In our case, this percentage is brought to a score on a scale of 0 to 5 (with 5 equivalent to 100%).

Usually, the vulnerability is assessed and used to calculate a risk value of an information system [2]. But in a cloud context, providers may be tempted to conceal their vulnerabilities for security reasons. This is why we use the coverage based on the security controls. By

using the maximum possible coverage value Covgmax (in our case 5), it is possible to get an equivalent to the vulnerabilities. Therefore, by combining this value with the harm we can define the following risk formula for a threat t, a cloud user k and a provider CSP p:

$$Risk(t,k,p) = Harm(t,k) + (Covg_{\max} - Covg(p,t)) \quad (2)$$

3) List Ranked of the Secured CSPs:

The CSBS model provides optimal cloud service provider selection from the more numbers of CSPs based on security risk values estimated in the last step which provides a list ranked of the more secured CSPs for each customer want to see the ranked results.

C. Recommendation Stage

After the risk evaluation stage, some of the user requests may fail to be matched to the appropriate provider. This failure likely originated in the fact that the users' requests and their matching providers are processed by different broker agents. In this case, a heuristic strategy is applied to seek another broker agent that has the most potential in brokering. The user agent will connect with this broker and start a new cycle.

A database is designed to handle the recommendation requests from broker agents. The broker agent attempts to make a suggestion by predicting the current advertised information of the provider agents based on their historical data in database. To implement this strategy, the broker agents periodically update the information about all of the provider agents connecting to it. The historical data represents the statistical pattern and provides the predictive information to the broker agent. The steps of recommendation are described as follows:

- After risk evaluation stage, broker agent 1 makes a list of requests of user agents connecting to it that failed to be matched.
- Broker agent 1 accesses the database to obtain a suggestion for the potential broker agent for each request.
- With each request, the broker agent looks into the risk value of providers to recommend another broker agent 2 that has the lowest risk value. The information about broker agent 2 will be sent back to the user agent by broker agent 1.
- The user agent will connect to broker 2 and starts a new cycle.

V. Implementation and Experiments Results

To demonstrate the feasibility and the efficiency of our approach, we illustrate a series of simulations using the architecture of the CSBS described in Section IV in case study with four cloud users CU 1, CU 2, CU 3 and CU 4 under some threats related to the CIANA objectives requesting services from five cloud providers X, Y, Z, T and W.

The security requirements step provides the needs of our customers using the user agents in terms of CIANA objectives (see Table 1). Then, the harm function on each cloud customer will be computed (see Table 2) and added to the coverage of the cloud providers for the 5 cloud threats (see Table 3) to obtain the maximum risk values corresponding to our cloud users for each provider by exploiting our CSBS functionalities in this case study.

TABLE I. SECURITY NEEDS OF THE FOUR CLOUD USERS

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity
CU 1	1	1	0	1	0
CU 2	0	1	1	1	1
CU 3	1	0	1	0	0
CU 4	1	0	0	1	1

TABLE II

CALCULATION OF THE HARM VALUES ON EACH CLOUD USER

	CU 1	CU 2	CU 3	CU 4
Data Breaches	1	0	1	1
Data Loss	1	2	1	1
Account Hijacking	3	4	2	3
Insecure Interfaces	2	2	1	2
Denial of Service	0	1	1	0

TABLE III

COVERAGE OF THE CLOUD PROVIDERS FOR THE 5 CLOUD THREATS

	CSP X	CSP Y	CSP Z	CSP T	CSP W
Data Breaches	3	5	4	1	2
Data Loss	5	3	4	4	2
Account Hijacking	1	4	3	2	5
Insecure Interfaces	2	5	5	1	3
Denial of Service	3	1	4	1	4

TABLE IV

MAXIMUM RISK VALUES OF THE CUS FOR EACH PROVIDER

	CSP X	CSP Y	CSP Z	CSP T	CSP W
CU 1	7	4	5	6	4
CU 2	8	5	6	5	7
CU 3	6	5	4	5	4
CU 4	7	4	5	6	4

Fig. 3 shows the comparison between the risks in cloud customers for the five cloud providers by using the broker agents presenting in our CSBS. Thus, the user can request services by starting with the providers having the minimum security risks [16].

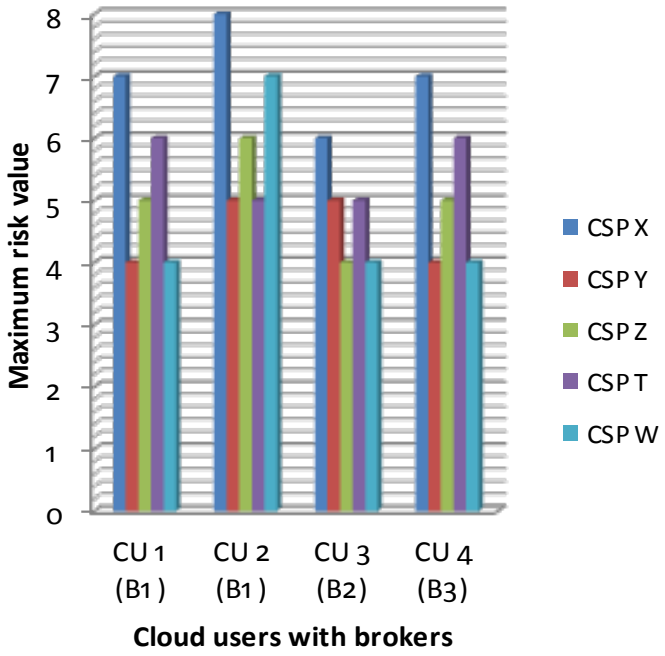

Fig. 3. Comparison of risks in cloud users for the five cloud providers

VI. Conclusion and Future Work

In this paper we have presented a MAS- based cloud service brokering system to respond the security needs of the cloud customers in the aim to deliver different types of services. So, the multiple cloud service providers make a dilemma for a cloud user to choose each provider is more secured and has the minimum security risk. Hence, we propose a cybersecurity model based on three stages used in the connection procedure of the cloud service brokering system. In this work, broker agents are introduced to make our approach more flexible and efficient which can handle a huge amount of user requests by implementing this system in a case study and comparing the empirical results. In the future, we plan to continue the current research work to allow CSBS to be extended in a real use cases, then combining the risk values with costs to make decisions for the cloud provider selection.

References

[1] M. Whaiduzzaman and A. Gani, "Measuring Security for Cloud Service Provider: A Third Party Approach", International Conference on Electrical Information and Communication Technology (EICT), pp. 1-6, 2013 IEEE.

[2] G. Elio, K. Dahman, and B. Gateau, C. Godart, "A Broker Framework for Secure and Cost-Effective Business Process Deployment on Multiple Clouds", CAiSE 2014 Forum/Doctoral Consortium, Thessaloniki, Greece. June 2014.

[3] Cloud Security Alliance. Cloud Control Matrix/Security, Trust & Assurance Registry/Consensus Assessments Initiative Questionnaire. Technical report.

[4] European Network and Information Security Agency. Benefits, risks and recommendations for information security. Technical report, 2009.

[5] D. Talia, "Clouds Meet Agents: Towards Intelligent Cloud Services", IEEE Internet Computing, Vol.16, pp. 78-81, 2012.

[6] J. Yan, R. Kowalczyk, J. Lin, M.B. Chhetri, S.K. Goh, and J. Zhang, "Autonomous Service Level Agreement Negotiation for Service Composition Provision", Future Generation Computer Systems, Vol. 23, No. 6, pp. 748-759, 2007.

[7] K.M. Sim, "Agent-based Cloud Computing", Services Computing, IEEE Transaction on, Vol. 5, No. 4, pp. 564-577, 2012.

[8] G. Linden, B. Smith, and J. York, "Amazon.com Recommendations: Item-to-Item Collaborative Filtering", IEEE Internet Computing, vol. 7, no. 1, pp. 76-80, Jan. /Feb. 2003.

[9] Z. Zibin, Z. Yilei, and M. R. Lyu, "Cloud Rank: A QoS-Driven Component Ranking Framework for Cloud Computing" in Reliable Distributed Systems, 29th IEEE Symposium on 2010, pp. 184-193.

[10] Z. Zheng, H. Ma, M. R. Lyu, and I. King, "QoS- Aware Web Service Recommendation by Collaborative Filtering", IEEE Trans. Service Computing, vol. 4, no. 2, pp. 140-152, Apr.-June 2011.

[11] P. Dhillon and V. Arora, "A Compositional Approach of Reliable and Efficient Cloud Service Selection", Volume 2, Issue 8, August 2012 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

[12] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS Ranking Prediction for Cloud Services", Parallel and Distributed Systems, IEEE Transactions on, vol.24, no. 6,pp. 1213-1222,June 2013.

[13] D. Kapgate, "Weighted Moving Average Forecast Model based Prediction for Service Broker Algorithm for Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 3, Issue. 2, February 2014.

[14] M. Subha and M. U. Banu, "A Survey on QoS Ranking in Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, February 2014.

[15] R. Yuvarani and M. Sivalakshmi, "Achieve Ranking Accuracy Using Cloud Rank Framework for Cloud Services", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Special Issue 1, March 2014.

[16] K. Amrutha and B. Madhu, "An Efficient Approach to Find Best Cloud Provider Using Broker", International Journal of Advanced Research in Computer Science and Software Engineering 4(7), pp. 943-946, July 2014.

[17] P. Bathla and S. Vashit, "A Sophisticated Study of QoS Ranking Frameworks in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 7, July 2014.

[18] M.T. Khorshed, A.B.M.S. Ali, and S.A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems, vol. 28, pp. 833-851, 6//2012.

[19] R. Buyya, Y. Chee Shin, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," in High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on, 2008, pp. 5-13.

[20] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Systems, vol. 25, pp. 599-616, 6//2009.

[21] S.M. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for the Cloud Computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on, 2011, pp. 933-939.

[22] J. Kang and K. M. Sim, "Towards Agents and Ontology for Cloud Service Discovery," 2011 IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

[23] C.P. Pfleegerc and S.L. Pfleeger, Security in Computing, 3rd edition, Prentice Hall, 2003.

[24] Cloud Security Alliance. Cloud Control Matrix / Security, Trust & Assurance Registry/Consensus Assessments Initiative Questionnaire. Technical report.

Jamal TALBI received the B.Sc. in Computer Sciences from the University of Hassan 1st, Faculty of Sciences and Techniques (FSTS), Settat, Morocco, in 2009, and M.Sc. degree in Business Intelligence from the Sultan Moulay Slimane University, Faculty of Sciences and Techniques (FSTBM), Beni Mellal, Morocco, in 2011. Currently, he is working toward his Ph.D. at FSTS. His current research interests include decision support, information systems, networking architectures, security, privacy, cryptography in cloud computing.

Abdelkrim HAQIQ has a High Study Degree (DES) and a PhD (Doctorat d'Etat), both in the field of modeling and performance evaluation of computer communication networks, from the University of Mohamed V, Agdal, Faculty of Sciences, Rabat, Morocco. Since September 1995 he has been working as a Professor at the department of Mathematics and Computer at the Faculty of Sciences and Techniques, Settat, Morocco. He is the Director of Computer, Networks, Mobility and Modeling laboratory and the responsible for engineering education in Computer Engineering at the same Faculty. He is also the General Secretary of the electronic Next Generation Networks (e-NGN) Research Group, Moroccan section. Dr. Abdelkrim HAQIQ is actually Co-Director of a NATO multi-year project and Co-Director of a Moroccan Tunisian research project. Dr. Abdelkrim HAQIQ's interests lie in the areas of modeling and performance evaluation of communication networks, cloud computing and security. He is the author and co-author of more than 80 papers (international journals and conferences/workshops). He was a publication co-chair of the fifth international conference on Next Generation Networks and Services, held in Casablanca, May, 28 - 30, 2014. He was also an International Steering Committee Chair and TPC Chair of the international conference on Engineering Education and Research 2013, iCEER2013, held in Marrakesh, July, 1st –5th, 2013, and a TPC co-chair of the fourth international conference on Next Generation Networks and Services, held in Portugal, December, 2 - 4, 2012. Dr. Abdelkrim HAQIQ was the Chair of the second international conference on Next Generation Networks and Services, held in Marrakech, July, 8- 10, 2010. He is also a TPC member and a reviewer for many international conferences. He was also a Guest Editor of a special issue on Next Generation Networks and Services of the International Journal of Mobile Computing and Multimedia Communications (IJMCMC), July-September 2012, Vol. 4, No. 3, and a special issue of the Journal of Mobile Multimedia (JMM), Vol. 9, No.3&4, 2014.