

An Agent-Based Cloud Platform for Security Services

Fernando De la Prieta^{1,*}, Luis Enrique Corredera², Antonio J. Sánchez-Martin¹,
and Yves Demazeau³

¹ University of Salamanca, Department of Computer Science and Automation Control, Plaza de la Merced s/n, 37007, Salamanca, Spain

{fer, anto}@usal.es

² Flag Solutions S.L., C/Bientocadas 12, 37002, Salamanca, Spain

luisenrique@flagsolutions.net

³ National Center for Scientific Research, Laboratory of Computer Science of Grenoble, Maison Jeat Kuntzmann – 110 av. De la Chimie, Gregoble, France

yves.demazeau@imag.fr

Abstract. There are many trials where electronic evidences are not digitally signed. This problem requires the validation of the veracity of these digital resources, thus causing delays in the verdict and increase the price of the process. The digital signature solves partially the problem because it provides the characteristics of authentication, integrity and non-repudiation; but it has weakness such as availability, confidentiality and changes control, besides the complexity on its usage. This paper presents the project DoyFE.es that is an agent-based platform deployed over a cloud system that provided cloud-based services to guarantee the veracity of the communications (email, web content and photographs).

Keywords: Multiagent systems, cloud computing, security, privacy.

1 Introduction

Nowadays, there are many trials where the evidences are based on electronic documents (files, information, emails, photographs, etc.). The majority of these documents have not been digitally signed, so it is difficult to validate their truthfulness. In these cases, it is necessary to validate the veracity of these evidences by means of forensic computer science techniques [3]. This process not only delays the trials, but also increases considerably their costs.

These problems can be *partially* addressed by the users through the use of the digital signature. Besides the electronic communications advantages, digital signed documents have many advantages facing to non-electronic one (i.e. authentication, integrity and non repudiation). But the problem is that the process of signing requires some configurations in the computers of the end-users that are complex for common users without a specific technical profile. This issue and the lack of awareness about digital signature advantages constitute an entrance barrier for this technology.

Although the European Commission is boosting the usage of the digital signature, its implantation is still limited¹. For example, in Spain there is a Law of Digital Signature² from 2003 that establishes different levels of digital signature and its legal equivalence with the traditional signature. However, the implantation of the digital signature is limited, following the statistical data of the Spanish Institute of Statistical³, as shown in Table 1 only the 24,36 % of the Spanish population have some methods of digital signature. In other words, only 11,5 millions of the 47 millions of Spanish have digital signature. But, the percentage of usage is even smaller, because, taking into account only the people that have these methods, only 4,7% use it in the case of eID and 13% in the case of other methods of signing.

Table 1. Usage of digital signature in Spain

	Have digital signature	Use eID	User other methods
Total	24,36 %	4,7 %	13,0 %
Men	52,17 %	5,1 %	14,3 %
Women	47,83 %	4,2 %	11,6 %

As we said, the digital signature deals partially with the problem, but there still are some weaknesses such as (i) *Availability*, it depends directly on the end-users because they are on charge of the backup of the signed document along the time; (ii) *Confidentiality*, it is not possible to monitor access to the signed files, so everyone would be able to see their content; and finally (iii), the Change Control, because when a signed document is changed, it is not possible to know what have been the changes.

This study presents the platform DoyFe.es⁴ that tries to solve these open issues. Not only those that are covered by the digital signature, but also the previously presented weaknesses (availability, confidentiality and change control). To do so, DoyFe.es platform exposes three cloud-based services for secure communication in order to ensure the tracking and secure storage of information exchanges and electronic transactions (procurements, shopping, etc.) in order to use this tracking information as evidence in a trial. DoyFe.es platform is based on Cloud Computing paradigm. Concretely, it is developed under +Cloud platform [6][11][8]. Thanks to that, it is possible to deal with the computational requirements and it also facilitates the commercialization following a payment model based on the usage (pay-as-you-go) [2]. The core of DoyFe.es is a multiagent system (MAS) based on virtual organization (VO)[17][7] that allows the interaction both with the underlying cloud platform and with the end-user.

This work is organized as follow, next section present the state of the art of the applications of agents under the frame of security and privacy. Then, Section 3 shows the three main developed services, while section 4 is focused the integration with the

¹ <http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

² Spanish Law 59/2003 –
<http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf>

³ <http://www.ine.es>

⁴ <http://www.doyfe.es/>

cloud platform and the MAS. Finally, last section contains the preliminary evaluation and conclusions.

2 Security Services in the Frame of Cloud Computing

Historically, the term Cloud Computing was first used by Professor Rammath. However [4], the concept was becoming popular through Salesforce.com, a company that focused its market strategy to offer software as a service (SaaS) to big companies. However, IBM was the first company to detail the specific terms of the guidelines of this technology (auto-configuration, auto-monitorization, auto-optimization) in the document Autonomic Computing Manifesto [12]. By 2007, Google, IBM and others had joined together to form a research consortium which resulted in the birth of this technology as we know it today [15]. For the large companies, knowledge about this technology is a competitive advantage. First of all, the Cloud provider can offer its services through a pay-as-you-go model following the guidelines proposed by Utility computing. Additionally, the Cloud user does not have to be concerned with demand peaks, transforming passive investments in operational expenses [2].

There are only a limited number of studies in the state of the art that relate Cloud Computing and agent technology [19]. However, some of them are related with security and privacy, these examples can be seen from two perspectives: (i) internal to cloud platform, in which they try to ensure the security of the underlying technology; and (ii) external, with examples that try to securize the communication links between the consumers and providers.

At external level, the studies are mainly related with the authentication of the stakeholders in a cloud platform. For example, the ABAC Project [22], or the client-side authentication model [10], as well as the work proposed by Habiba et al. [9] in which a MAS uses different policies for grant privileges over the information. At internal level, the studies are focus in guarantee the privacy of the data [5], the monitoring of the system, [16] the security of the infrastructure (real/virtual) [14] and, finally, some works related with the safe storage such as CloudZone [20], Prometheus methodology [21], multilayer security model [13] and so on.

In the state-of-the-art it is not possible to find relevant works about cloud-based services focus on the tracking of the communications in order to use this log as evidence within a trial.

3 Cloud-Based Security Services

Under the frame of DoyFe.es project a set of services has been developed in order to guarantee the authentication, integrity and non-repudiation, but also other open issues such as availability, confidentiality and change control. To do so, three main services has been created: (i) an embedded web browser (*browser-in-a-browser*) focuses on providing of third-party guarantee about transactions and communications done in Internet; (ii) mobile application to take and certify the veracity photographs (iOS and Android); and (iii) an email active gateway to certify the exchange of this kind of

communications. The main advantage of these services is their simplicity because the user does not have to install nothing or to set up complex configurations.

The main aim of these services is to track all the communication and store it in order to use them when the end-user needs them. This tracking can be use as evidence in a trial with a third-party certification of its truthfulness. All the information about these services and the evidences is available to the end users in a web application. It makes possible the commercialization of the evidences (web content, photographs and emails) following a usage-based pay model.

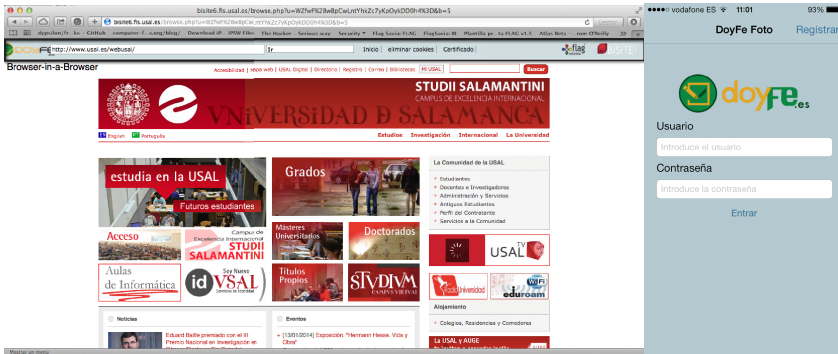


Fig. 1. Right: Browser in a browser; Left: Mobile application

3.1 Transmission and Signed Backup of Emails

Figure 1 shows an overview of transmission and receipt of emails within DoyFE.es. An active inbox model is used to facilitate the usability of the system. The process is very easy, because the end-user sends the email normally and only has to put in copy a special email of the platform (doyfe@doyfe.es). With this email in copy the platform also receives it in order to process it. The processing includes the signing, time-stamped and the storage of the data this email (content, dates, addresses, headers, etc.). After that, DoyFe.es sends a proof of the evidence to the sender and recipients.

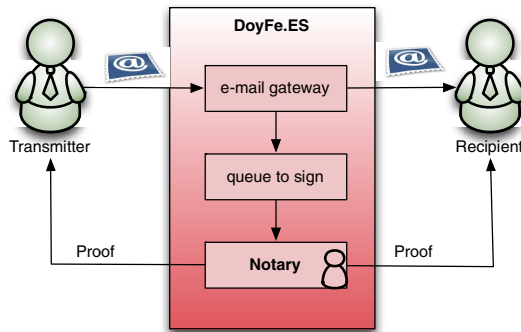


Fig. 2. Transmission and receipt of emails

3.2 Transmission and Signed Backup of Web Content

The process of tracking (signing and storage) of web content is more complex because the web pages usually include related contents (i.e. images, style sheets, javascript, etc.). So, it is needed not only to process the main content (usually pages written in HTML), but also all related content and all exchanges of request and responses.

The process is similar to the email but due the large amount of files and contents it requires more time of processing. Finally, DoyFe.es takes a screenshot of the full webpage in order to avoid the different visualizations that depend on the specific browser.

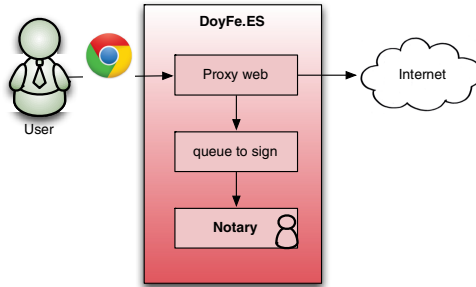


Fig. 3. Process of taking evidences in web browsing

3.3 Signed of Photographs

The process of tracking photographs is different because it is not only necessary to sign the taken photography by a mobile phone, but also geolocalize it. Also, a second photography with the frontal camera is taken in order to know who is the person that takes the photography. This second evidence completes the information related with the electronic evidence.

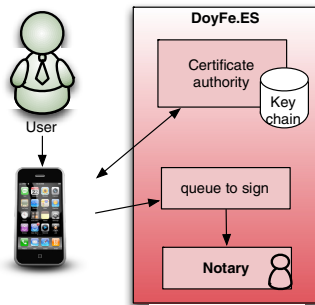


Fig. 4. Process of sign images and their information

In previous services the files are signed within the cloud platform, but in this case they are signed into the mobile phone. To do so, it is necessary to exchange information between the cloud platform and the phone about the security certificate. Once the mobile phone has a valid certificate, the process of sign is similar to the previous ones and then the signed documents are uploaded on the platform.

4 DoyFE Platform

Once the communication services have been presented, there is no doubt that their nature requires large computational resources (CPU and persistence). DoyFE.es not only has to store large amount of information, but also it needs computational power to sign the files in order not to delay the normal flow of the signed resources.

Thus, DoyFe.es platform is deployed over +Cloud which is a cloud-based platform [6][11][8] that used a CBR (Case-Based reasoning) to control the elasticity of the services, the model of CBR has used satisfactorily on environments with uncertainty [1][18]. The CBR is a previously using in uncer. This platform allows offering services at the PaaS and SaaS levels:

- The **FSS (File Storage Service)** provides an interface to a file container, emulating a directory-based structure, in which the files are stored with a set of metadata thus facilitating retrieval, indexing, searching, etc.
- The **OSS (Object Storage Service)** is a document-oriented and schemaless database service, which provides both ease of use and flexibility. In this context, a document is a set of keyword-value pairs where the values can also be documents (is a nested model), or references to other documents (with very weak integrity enforcement).

Both services are presented in the form of stateless web services (REST in API format). The data format used for communication is JSON, which is more easily readable than XML and includes enough expression capability for the present case.

The internal layer is used to deploy all management and general-purpose applications, in addition to the all services at the platform layer, such as the services offered by DoyFE.es. This layer provides a virtual hosting service with automatic scaling and functions for balancing workload. It consists of a set of physical machines which contribute to the system by means of their computational resources. Abstractions are performed over these hardware resources, as virtual machines, which allows the easy and dynamic management of computational resources. +Cloud platform uses virtual organizations of agents to manage the system resources. MAS can be perfectly adapted to solve this problem, as it allows making decisions in an open environment where the availability of information is limited and agents are thereby required to make decisions, amidst great uncertainty, that affect the entire system.

Under the frame of DoyFE.es, the persistence services at PaaS level (FSS and OSS) represent the *Digital Repository* where the signed documents are stored. But also, +Cloud provides a deployment environment where the computational power (needed for signing) is taken from the virtual machines where each service is deployed. DoyFE.es is also based on VO of MAS that controls the task, signed process, interactions among components, as well as the interaction with +Cloud in order to control the resources requested by the platform.

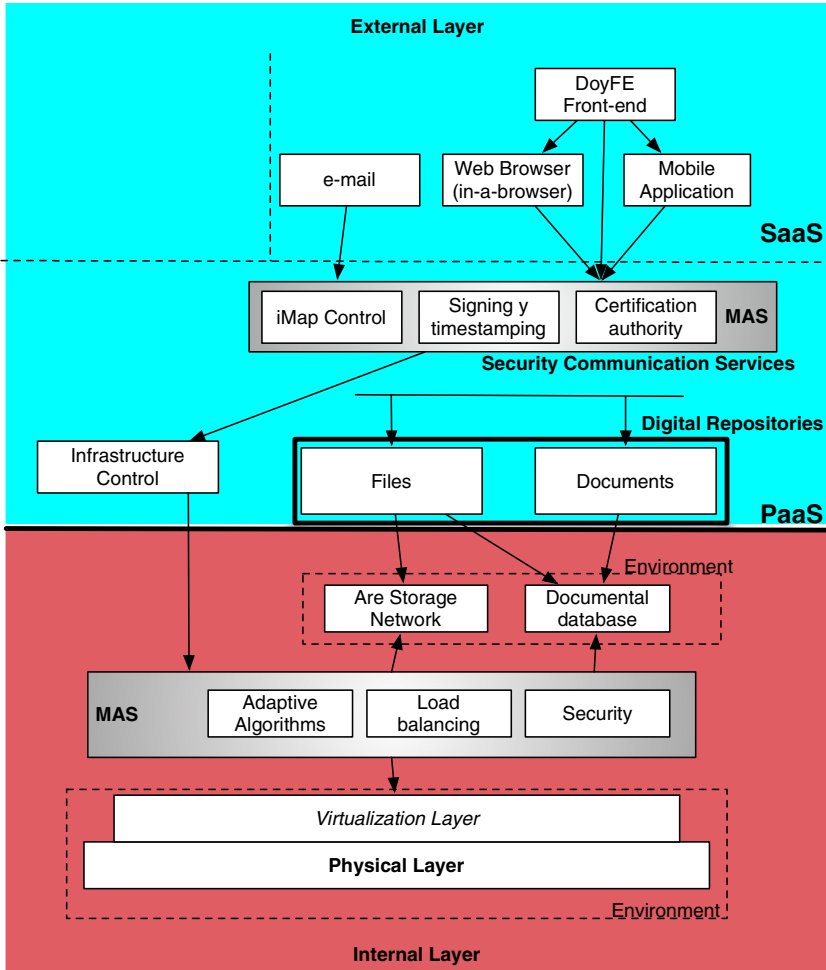


Fig. 5. Components diagram of DoyFE.es

4.1 The Core: A Multiagent System Based on Virtual Organizations

As it is explained in [6], the core of +Cloud is based on two virtual organizations as follow:

- Resource Organization.** This agent organization is charge of managing both the physical and virtual system resources. The agents are distributed throughout the hardware elements of the Cloud environment. Their main goal is to maximize the use of resources. It is intended that there are no active resources that are underutilized, which implies that there must be the smallest possible number of active physical machines to satisfy the current demand. To do that there is a role to monitor each physical server (*Local Monitor*), a role to control each physical

server (*Local Manager*) and finally another role to control the allocation of resources and among different physical servers (*Global Manager*), for example operations such as instantiating virtual machines, migrating, etc.

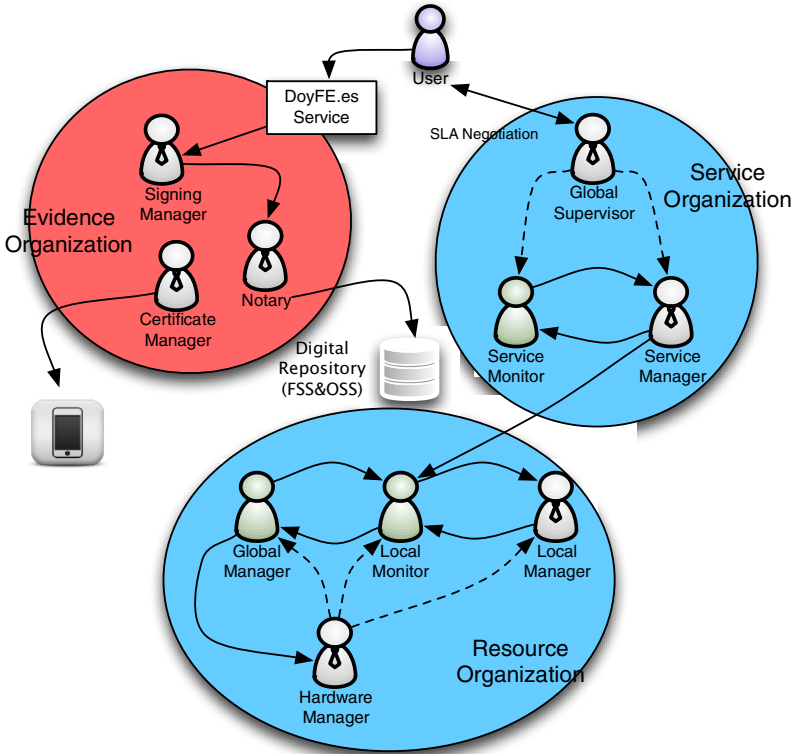


Fig. 6. Organizations of agents in DoyFe.es y+Cloud

- Consumer Organization.** At the technological level this organization deploys over the computational resources offered by the organization described in the previous section. The services encompassed by this organization will, therefore use the system resources according to existing demand. Its main goal is to maximize the quality of service, which requires monitoring each service individually, keeping in mind that each service will be deployed simultaneously on various virtual machines located in different physical services. The roles within this organizations are the following: the (i) *Service Monitor* that balances between the virtual machines the load and it also monitors each service in terms of quality, the (ii) *Service Manager* that controls each services and alerts to Local Manager when the quality of the services is not enough. These two services take care of all deployed services over +cloud, including the specific communication services at PaaS and SaaS level developed under the frame of DoyFe.Es. Additionally, there is another role, (iii) *Global Supervisor* that takes

care about the negotiation of SLA (Service Level Agreement) and their surveillance of those reached with the end-users in order to fulfill with them.

DoyFe.ES incorporates an additional organization in order to manage the evidences, this organization include three main roles:

- **Signing manager.** It is in charge of gather the information for signing, converts it into the appropriate format and sends it to the Notary for signing. It also tests that the information fulfills with the requirements that are need to be signed. Once the Notary signs the information, this role checks that the signing process has been done correctly and then it stores the information in the Cloud.
- **Certificates manager.** It manages the creation, store and revocation of digital certificates. There are two types of certificates: for the mobile clients (to use them in the mobiles phones), and for the notary agents (to use them within the platform).
- **Notary.** It is the role that sign the documents received from the Signing manager, using the keys provided by the Certificate manager.

The main advantage is the combination of both platforms because they are based on MAS and it is easy to exchange of information between DoyFE.es and +Cloud. While the user negotiates the SLA directly with +Cloud, DoyFe can send alerts about the performance of the signing process.

5 Preliminary Evaluation and Conclusions

Once the DoyFE.es and its integration with +cloud are presented, this section focuses on the preliminary evaluation of the overall system. Firstly, the first test is oriented to evaluate the performance of DoyFE.es (without +Cloud). The system has to produce signed files without delaying the normal usage from the user point of view. Following we presented a test that was performed to the heaviest service which is the service oriented to track the web content navigation. The test consists in the comparison of the time load of 60 websites, randomly chosen, using the tool GNU WGET⁵. As it shown in Table 2, the load time using the solution of DoyFE.es, which is a browser in a browser, is acceptable because the process of signing only delays the navigation around a 20% over the normal use.

Table 2. Average of website load with and without (DoyFe.es)

Size	Normal load	Load with DoyFE.es
< 1 Mb	2,42 s	3,13 s
1-3 Mb	4,05 s	5,20 s
> 3	7,08 s	8,62 s

The main advantage of DoyFE.es is to be deployed over a Cloud Computing environment and the easiness of the exchange information between both systems. Moreover, the end user has a perspective of a single system, however, the reality is that the

⁵ <http://www.gnu.org/software/wget/>

users make use of the services of DoyFE.es and the computational power of +Cloud, besides the negotiation of SLA are managed directly with the cloud platform. To validate the integration, tests to measure the performance of the DoyFE.es' services after the integration. Table 3 shows the load time average of reference website (<http://bisite.usal.es>) using the browser-in-a-browser service of DoyFE.es with and without its integration in +Cloud. As this table shows the average are better using +cloud, as expected.

Table 3. Comparison between DoyFE.es and its deployment in +Cloud

Current users	DoyFE.es	DoyFE.es in +Cloud
100	4,81 s	4,02 s
1000	7,40 s	4,84 s
10000	19,54 s	5,52 s

During this study we have demonstrated not only the correct operation of DoyFE.es platform, but also its possible application with the legal frame in order to validate the genuineness of the electronic evidences by a third party using an innovative perspective and traditional tools such as digital signature and service. However if we think beyond, the integration of this system within a cloud computing platform increases notably the performance of the communication services.

We are also demonstrating that the development of an agent-based cloud computing platform has many advantages because it makes easy the interaction with the environment (deployed services, users, other clouds, etc.) in order to give better services to the end-user. In this sense, our open lines are focused on this interaction between both systems, combining the usage information of services (PaaS and SaaS) with their requested resources, in order to achieve the goal of efficiency within the cloud platforms paradigm.

Acknowledgements. This research has been partially supported by Spanish Centre for Industrial Technological Development (CDTI) through the project DoyFE.es (ID-20120798)

References

1. Bajo, J., Corchado, J.M.: Evaluation and monitoring of the air-sea interaction using a CBR-agents approach. In: Muñoz-Ávila, H., Ricci, F. (eds.) ICCBR 2005. LNCS (LNAI), vol. 3620, pp. 50–62. Springer, Heidelberg (2005)
2. Buyya, R.: Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. In: 10th IEEE International Conference on High Performance Computing and Communications, HPCC 2008, pp. 5–13 (2008)
3. Casey, E.: Digital evidence and computer crime: Forensic science, computers, and the internet. Access Online via Elsevier (2011)
4. Chellappa, R.: Intermediaries in cloud-computing: A new computing paradigm. In: INFORMS Dallas 1997 Cluster: Electronic Commerce, Dallas, Texas (1997)

5. Damiani, E., Pagano, F.: Handling confidential data on the untrusted cloud: an agent-based approach. arXiv preprint arXiv:1012.0759 (2010)
6. De la Prieta, F., Rodríguez, S., Bajo, J., Corchado, J.M.: A Multiagent System for Resource Distribution into a Cloud Computing Environment. In: Demazeau, Y., Ishida, T., Corchado, J.M., Bajo, J. (eds.) PAAMS 2013. LNCS, vol. 7879, pp. 37–48. Springer, Heidelberg (2013)
7. Gómez-Sanz, J.J., Pavón, J., Garijo, F.: Meta-models for building multi-agent systems. In: Proceedings of the 2002 ACM Symposium on Applied Computing, pp. 37–41 (2002)
8. González, R., Hernández, D., De la Prieta, F., Gil, A.B.: +Cloud: An Agent-Based Cloud Computing Platform. In: Omatu, S., Neves, J., Rodriguez, J.M.C., Paz Santana, J.F., Gonzalez, S.R. (eds.) Distrib. Computing & Artificial Intelligence. AISC, vol. 217, pp. 377–384. Springer, Heidelberg (2013)
9. Habiba, M., Islam, M., Ali, A.B.M.: Access Control Management for Cloud. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 485–492. IEEE (July 2013)
10. Hajivali, M., Fatemi Moghaddam, F., Alrashdan, M.T., Alothmani, A.Z.: Applying an agent-based user authentication and access control model for cloud servers. In: 2013 International Conference on ICT Convergence (ICTC), pp. 807–812. IEEE (October 2013)
11. Heras, S., De la Prieta, F., Julian, V., Rodríguez, S., Botti, V., Bajo, J., Corchado, J.M.: Agreement technologies and their use in cloud computing environments. *Progress in Artificial Intelligence* 1(4), 277–290 (2012)
12. Horn, P.: Autonomic Computing: IBM's perspective on the State of Information Technology. IBM Manifesto (October 2001), http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf (last visited: January 2014)
13. Islam, R., Habiba, M.: Collaborative swarm intelligence based Trusted Computing. In: 2012 International Conference on Informatics, Electronics & Vision (ICIEV), pp. 1–6. IEEE (May 2012)
14. Li, Z., Chen, C., Wang, K.: Cloud computing for agent-based urban transportation systems. *IEEE Intelligent Systems* 26(1), 73–79 (2011)
15. Lohr, S.: Google and ibm join in cloud computing research. *New York Times* (October 2007), RI: http://www.nytimes.com/2007/10/08/technology/08cloud.html?_r=0
16. Pal, S., Khatua, S., Chaki, N., Sanyal, S.: A new trusted and collaborative agent based approach for ensuring cloud security. arXiv preprint arXiv:1108.4100 (2011)
17. Rodríguez, S., de Paz, Y., Bajo, J., Corchado, J.: Social-based planning model for multi-agent systems. *Expert Systems with Applications* 38(10), 13005–13023 (2011)
18. Sánchez-Pi, N., Carbó, J., Molina, J.M.: A Knowledge-Based System Approach for a Context-Aware System. *Knowledge-Based Systems* 27, 1–17 (2012)
19. Talia, D.: Clouds meet agents: Toward intelligent cloud services. *IEEE Internet Computing* 16(2), 78–81 (2012)
20. Talib, A.M., Atan, R., Abdullah, R., Murad, A.: Security framework of cloud data storage based on Multi Agent system architecture-A pilot study. In: 2012 International Conference on Information Retrieval & Knowledge Management (CAMP), pp. 54–59. IEEE (March 2012)
21. Talib, A.M., Atan, R., Abdullah, R., Murad, M.A.A.: Multi Agent System Architecture Oriented Prometheus Methodology Design to Facilitate Security of Cloud Data Storage. *Journal of Software Engineering* 5(3), 21 (2011)
22. Venkataramana, K., Padmavathamma, M.: Agent Based approach for Authentication in Cloud. *IRACST-International Journal of Computer Science and Information Technology & Security* 2(3), 598–603 (2012)