Security services as cloud capabilities using MAS

Fernando De la Prieta, Alberto López Barriuso and Juan M. Corchado
Universidad de Salamanca, Departamento de Informática y Automática, Plaza de la merced s/n, 37007, Salamanca (España)
{fer, albarriuso, corchado}@usal.es
Luis Enrique Corredera de Colsa
Flag Solutions S.L., C/Bientocadas 12, 37002, Salamanca, (España)
luisenrique@flagsolutions.net

***Abstract*- The digital signature solves partially the problem of the validation of veracity of the digital resources because it provides the characteristics of authentication, integrity and non-repudiation. However, it has weakness in terms of 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 provides cloud-based services to guarantee the veracity of the communications (email, web content and photographs).**

This work has been previously published:

De la Prieta, F., Corredera, L. E., Sánchez-Martin, A. J., & Demazeau, Y. (2014, January). An Agent-Based Cloud Platform for Security Services. In PAAMS (Workshops) (pp. 333-343).

I. INTRODUCTION

Nowadays, there are many trials where 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 [1]. 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).

Despite the use of digital signature, there still are some weaknesses in terms of (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 what were the changes.

This study presents the platform DoyFE.es[1] that deals with these open issues. To do so, DoyFe platform exposes three cloud-based services for secure communication of information exchanges and electronic transactions. DoyFe is based on Cloud Computing (CC) [2][3], which improves the commercialization following a payment model based on the usage [4]. The core of DoyFe is a multiagent system (MAS) based on virtual organization (VO) [5] that allows the interaction both with the underlying cloud platform and with the end-user.

This work is organized as follow, next section presents the three main developed services, while section 3 is focused on the integration with the cloud platform and the MAS. Finally, last section contains the conclusions.

II. 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 have been created:

- **Transmission and signed backup of emails.** 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). The processing includes the signing, timestamped and the storage of the email data (content, dates, addresses, headers, attachments, images, etc.).
- **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, scripts, etc.). So, it is needed not only to process the main content, but also al related content and all exchanges of request and responses.
- **Sign 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. A second photography with the frontal camera is taken in order to know who is the person that takes the photography. To do so, the user has to install a specific APP. 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 because the photograph is signed on the smartphone.

[1] http://www.doyfe.es/

III. DOYFE PLATFORM

Once the communication services have been presented, there is no doubt that their nature requires large computational resources. DoyFE not only has to store a large amount of information, but also needs computational power to sign the files in order not to delay the normal flow of the signed resources. Thus, DoyFe platform is deployed over +Cloud which is a cloud-based platform [2][3] that used a CBR (Case-Based reasoning) to control the elasticity of the services. This platform allows offering services at the PaaS and SaaS levels. Under de frame of DoyFE (Fig. 1), the persistence services at PaaS level 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.

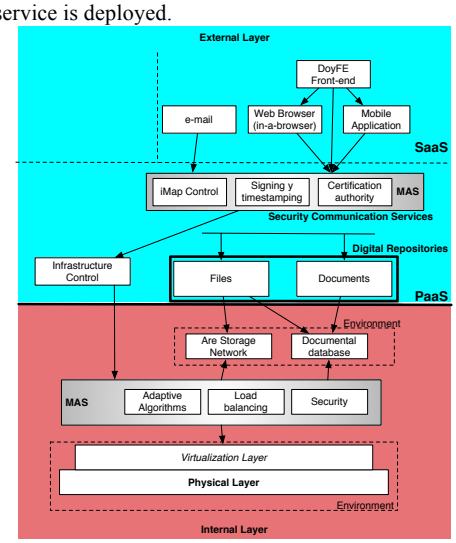

Fig. 1. Components diagram of DoyFE.es

+Cloud platform uses VO to manage the system resources (Fig. 2). 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. 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. Its main goal is to maximize the use of resources.
- **Consumer Organization.** 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.

DoyFe incorporates an additional organization (Fig. 2) in order to manage the evidences, this organization include three main roles:

- **Signing manager.** It is in charge of gather the information for signing and converts it into the appropriate format and sends it to the *Notary* for signing.
- **Certificates manager.** It manages the creation, store and revocation of digital certificates for mobile clients and for the notary agents.
- **Notary.** It is the role that signs the documents received from the *Signing manager* using the keys provided by the Certificate manager.

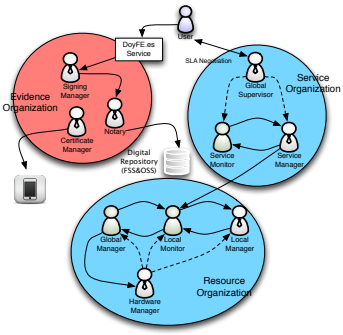

Fig. 2. Organizations of agents in DoyFe.es y +Cloud

IV. CONCLUSIONS

The main advantage of DoyFE.es is related with the fact of it is deployed over a CC platform. Moreover, the end user has a perspective of a single system, however, the reality is that the users make use of the services of DoyFE and the computational power of CC. Moreover, it is possible to use DoyFE within 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.

Acknowledgements. This work has been supported by the SOHA+C project (Ref. SA213U13) funded by Junta de Castilla y Leon.

REFERENCIAS

[1] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

[2] De la Prieta, F., Rodríguez, S., Bajo, J., & Corchado, J. M. (2013). A Multiagent System for Resource Distribution into a Cloud Computing Environment. In *Advances on Practical Applications of Agents and Multi-Agent Systems* (pp. 37-48). Springer Berlin Heidelberg.

[3] Heras, S., De la Prieta, F., Julian, V., Rodríguez, S., Botti, V., Bajo, J., & Corchado, J. M. (2012). Agreement technologies and their use in cloud computing environments. *Progress in Artificial Intelligence*, *1*(4), 277-290.

[4] Buyya, R. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. 10th IEEE International Conference on High Performance Computing and Communications, 2008. HPCC '08. Pages. 5-13

[5] Rodríguez, S., de Paz, Y., Bajo, J., Corchado, JM. Social-based planning model for multiagent systems. Expert Systems with Applications 38 (10), 13005-13023. 2011.