Toward a Privacy Enhancing Framework in E-government

Wiem Hammami[1], Lamjed Ben Said[1], Sameh Hadouaj[1], François Charoy[2], Khaled Ghedira[1],

[1] Intelligent Information Engineering Laboratory
Higher Institute of Management of Tunis
41, Rue de la Liberté, Cité Bouchoucha 2000 Le Bardo, Tunis, Tunisia
[2] Loria, Lorrain Research Laboratory in Computer Science and its Applications
Campus Scientifique, 54506 Vandoeuvre-lès-Nancy, Cedex, France,
{lamjed.bensaid, khaled.ghedira}@isg.rnu.tn, hadouaj@yahoo.fr,
wiem.hammami@ymail.com, Francois.Charoy@loria.fr

Abstract. E-government involves data sharing between different partners such as citizens and government agencies. Thus, the use of personal data in such cooperative environment must be done in legal ways and for legal purposes. In this context, issues related to data protection, such as privacy, have to be considered. This paper adopts a multi-agent based approach to manage privacy concerns in e-government systems. The proposed model provides a mechanism for e-government systems to evaluate trust degree reached by digital government processes. For this purpose, concepts of responsibility proposed in multi-agent systems and access rights used in security models, are integrated in this work. The research provides an evaluative framework for trust degree related to e-government process.

Keywords: E-government, privacy, trust, multi-agent systems, simulation.

1 Introduction

Privacy refers to the ability of individuals to control the collection, retention, and distribution of information about themselves [1]. In the context of e-government, privacy is a critical issue as there is an increased amount of private data shared between different agencies. For example, to access public service online, citizens must fill in some forms that require Personally Identifiable Information (PII) such as name, social security number, credit card number, etc. Citizens need to know whether their PII are used in the right way and for the right purpose or not. This can be achieved by an enhanced ability of control over their personal information. In this paper, we focus on data privacy, in particular, on privacy protection of personal data exchanged, processed and stored in e-government systems. As citizens act at the front office side of the e-government system, they do not know what happens to their personal information handled in the back office side by government agencies. Agent technology can be a suitable solution for this situation as they can act on behalf of the

user. An agent is a computer system situated in some environment, and that is capable of *autonomous* actions in this environment in order to meet its design objectives [2]. The main issue of this paper is to propose a mechanism to control the use of personal information by e-government agents based on restrictions imposed on their behavior and to evaluate the trust degree related to e-government process.

The rest of this paper is structured as follows. In the second section we present different visions for privacy protection in the literature. In section 3 we describe our proposed model including the fundamental concepts used and their formal representations. Section 4 is devoted to experimentations and simulation results. In section 5, we make a comparative study of our work with other proposed model in the literature. Finally, section 6 summarizes the contribution of this work, and provides conclusions and future work.

2 Related works

Many approaches have been used to manage privacy concerns. We specially note those based on users preferences such as the P3P (Platform for Privacy Preferences) [3]. P3P provides technical mechanism to inform web sites users about privacy policy before they release their personal information. However, P3P does not provide mechanism for ensuring that sites act according to their policies [4]. Additionally, we mention approaches based on security modeling such as the Access Control Decision System. We note for example, the Role-Based Access Control model (RBAC) [5] that manages privacy through access control systems. In RBAC, users are assigned to roles to have permissions that allow them to perform particular job functions. However, we regret the lack of mechanism ensuring privacy protection of data after their collection in both P3P and RBAC approaches.

There are also a number of agent based privacy schemas in the literature. We note Hippocratic Multi-Agent Systems (HiMAS) [6]. HiMAS model define the concept of private sphere of an agent or a user that enable to structure and to represent data involved in privacy management. However, HiMAS model do not define metrics for trust evaluation. We note that existing approaches are often concerned about privacy protection in the data collection phase. But, actually we need to control data after their collection by e-government systems. Our main contribution is that we propose a new privacy schema based on multi-agent systems to handle such drawbacks of the existing knowledge.

3 The Privacy Enhancing Model

In this section, we introduce our multi-agent based model that we call ABC (Agent-Based Control). First, we describe the concepts used. Then, we present the ABC mechanism, and finally we describe our proposed techniques.

The ABC model enables to manage privacy concerns in e-government systems. This model offers a mechanism based on the use of a set of privacy rules and a set of information on the parties' rights, roles, responsibilities and restrictions to make a

statistical assessment of *trust*. Consequently, ABC model enables the subsequent authorizations to transfer private data.

3.1. Model description

In the ABC model (see Fig. 1), we define two kinds of agents: *Admin agents* and *AP agents* (Authorization Provider agents). Admin agents represent the staff working in government agencies. AP agents are charged to provide *authorizations* to Admin agents in order to communicate with each other or to access objects in the system. Each Admin agent in our model plays a set of *roles* (e.g. the tax controller, the mayor, etc). A role includes a set of *responsibilities* (e.g. mayor roles: sign documents, validate, etc) that are restricted by *access-rights* (e.g. read only, write, read-write, etc). These access-rights are used to protect the *resources* and they are managed by a set of *privacy rules*. Access rights are also justified by a specific *context*. In fact, what is appropriate in one context can be a violation of privacy in another context.

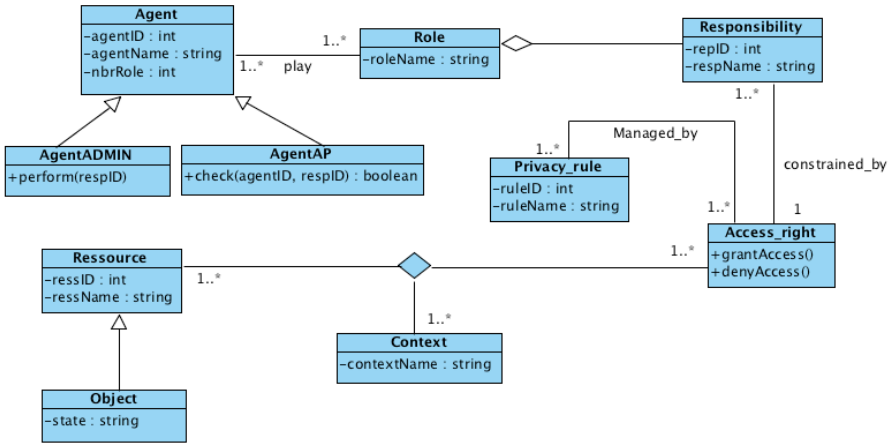

Fig. 1. ABC model

3.1.1. Definition of agent responsibility

We define responsibilities as the restricted behavior of a given agent. In other words, responsibility is the behavior that the system expects from an agent based on *restriction rules* (RR). We note that restriction rules are used to manage agent behavior at an internal level (e.g. making temporary results in a standard format before continuing execution, requesting specific authorizations before performing some actions, etc.). To more explain the concept of responsibility, let's take this example: we suppose that A_1 is an agent responsible for sending e- mails to agent A_2 (we suppose that e-mails are confidential). When we observe A_1's behavior, we find that A_1 sends e-mails to agent A_2 and sends a copy to the agent A_3 at the same time.

Thus, A_1 in this case did not assume his responsibility as some restriction rules are not respected.

3.1.2. Definition of privacy rules

Citizens must have control over their personal information handled by government systems. The Fair Information Practices (FIPs) [7] is an example of control enhanced by legislation, such as: limiting collection and disclosure, identifying purposes, etc.

In the ABC model, we define the following privacy rules that are in compliance with the FIPs and considered as the core needed to test and apply ABC model:

- *R1: each agent must assume his responsibilities.*
- *R2: each agent has access only to objects needed for doing the set of his responsibilities.*
- *R3: agent cannot use the context to access linked data outside the set of his responsibilities.*

For the privacy rules specifications, we are based on the notation of the rule-based systems [8] used in artificial intelligence, such that:

R1: Agent (A) ∧ Responsibility (Re) ∧ Responsible-for (A,Re)→Authorization(A, Re)

R2: Responsible-for (A,Re) ∧ Access (R,O,Re)→ Authorization(A, Re, R,O)

R3: Responsible-for(A,Re)∧Access(R,O,Re)∧(O→J) → NOT(Authorization(A,Re, R,J)

3.2. Description of ABC mechanism

In the ABC model, we define a distributed architecture in which sets of the agent in different groups are interacting with each other. Each group (container) represents the set of Admin agents running in the same e-government agency. To have access to objects in the system or to communicate with other agents, each Admin agent must be authorized from AP agent that exists in his group. To keep control of the system, AP agents use a Rule Base (RB) and a Knowledge Base (KB). RB includes the set of privacy rules and KB includes the set of knowledge in the system: agents, their roles, their responsibilities, their RR, their access-rights and their resources. In ABC model, we suppose that in case of failure, AP agents can switch roles dynamically with Admin agents. AP agents delegate the control of the system to the most trusted Admin agent. This delegation decision is based on the computation of Admin agent's honesty degree that will be explained in the next section.

3.3. Description of ABC techniques

In this section, we define techniques used for privacy protection in ABC model: the computation of the trust and the honesty degrees. Formally, our ABC model correspond to the following set: {A, Re, Au, PR, T, R} such that:

A: the set of agents in the system
Re: the set of agent responsibilities
Au: the set of authorizations
PR: the set of privacy rules

T: the trust degree reached in an e-government process. T is defined as*:*

$$T = \sum_{\substack{i=1 \\ i \neq j}}^{k} h(i,j) * \alpha_j / k. \quad (1)$$

where *k* represents the total number of agents in the system, *h* represents the honesty of agent j estimated by agent i (see Fig. 2). *h* is defined as follows:

$$h = \sum_{i=1}^{i=k} h(i,j). \quad (2)$$

After each transaction, an Admin agent i can give feedback to Admin agent j according to the service quality of j. Thus, a feedback score S is calculated as follows: S= P-N, where P is the number of positive feedbacks left by agents and N is the number of negative feedbacks from agents. The S value is disclosed to all agents in the system. This reputation model has been presented in [9]. *h* is decreasing when the agent is performing unauthorized actions. We define two types of such actions: unauthorized access to objects, and unauthorized communications with other agents. We suppose that honesty value is between 0 and 1 and it is disclosed to all agents in the system. α_j represents the interaction degree related to agent j. it denotes a weight used to balance T value because we must consider that agents behave differently. In our model, honest agents (having h=1) are rewarded. However, dishonest agents (having h<0,5) are punished.

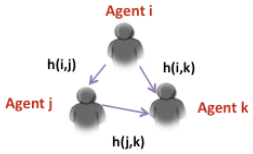

Fig. 2. Representation of Admin agent's honesty

We represent risk degree associated to the use of personal information (R), by the following:

$$R = 1\text{-}T \cdot \quad (3)$$

4 Simulation and experimental results

Using agent technology, we can make *« behavioral simulation »* that enable us to create a virtual image of the reality. This is considered as a powerful predictive analysis tool that enable decision makers to test their idea via scenario in an artificial environment before implementing their decision in the real world. In this section, we present our Multi-Agent Based Simulation (MABS) of agents' behavior during the company formation process in Tunisia. We chose this scenario because it is complex (involves numerous administrations and many interactions) and requires the collection

of many sensitive data at every step. We represent governmental agencies involved in this process by a set of agents (twelve agents) interacting with each other on behalf of the user (the citizen) and we simulate their behavior during the whole process using the ABC model. Our MABS is implemented using JADE platform [10]. We used JADE because it is a distributed platform and supports agent mobility. The mobility is an important issue of our work for a real application of the proposed model. For the privacy rules' specifications, described in section3, we used the rule engine Jess [11] to make authorization' decision based on both agent's responsibilities and access rights. To realize our simulation, we made the following hypothesis:

- All agents initially are honest (having h = 1)
- A simulation step corresponds to n successive interactions. In the following simulation results, we assume that n=10.

At every simulation step, we evaluate Admin agent's honesty and the trust value.

The first experimental result is the evaluation of trust degree reached during the running of company formation process. The trust (versus the risk) degree obtained during nine steps of our simulation is plotted in Fig. 3.

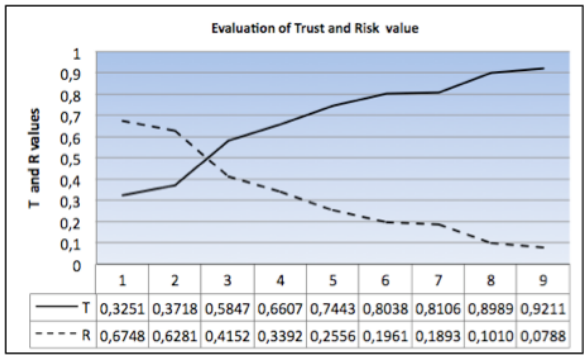

Fig. 3. Evaluation of Trust (T) and Risk (R)

As observed, we note that T is increasing notably during the simulation and R is decreasing (as there is a dual relation between T and R).

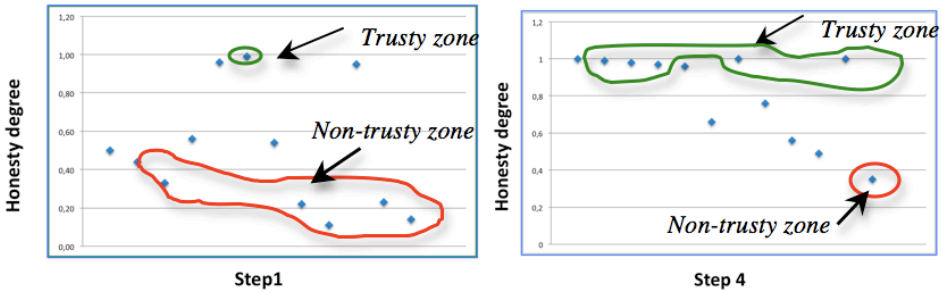

Fig.4. (a) Comparison of agent's honesty in step1, (b) Comparison of agent's honesty in step 4

According to our model, honest agents (having h=1) are placed in a trusty zone and dishonest agents (having h<0,5) are placed in non-trusty zone. As shown in Fig. 4 (a), we note that in the first step of our MABS only one agent is honest. However, when we observe agent's behaviors during next steps, we note that the number honest agents increase (Fig. 4 (b) shows an example of this increase during the step 4 of our MABS).

According to this interpretation, we find that agents placed in the non-trusty zone want to behave like honest agents, they want to move to the trusty zone. This enabled us to interpret the increase of the trust value during the simulation.

5 A comparative study

Regarding to some standard evaluation criteria, such as the use of access control mechanisms, the use of user preferences, the trust evaluation metrics [12] and the use of anonymity techniques [13] our work is the most appropriate one that is able to support all of these criteria. The following table summarizes the comparative study of our model with P3P and RBAC models. For each criterion we attribute (+) to the model that supports it and (-) to the model that does not support it.

Table 1. A comparative study

Evaluation criteria	Related works (1) RBAC	Related works (2) P3P	Our work ABC
Access control	+	-	+
User preferences	-	+	+
Trust evaluation metrics	-	-	+
Anonymity	-	-	+

In fact, the use of agent technology in our work, has many advantages:
Agent-based models provide a more convincing approach to modeling the real world behaviors due to their ability to explicitly model a component of the real world such as: human, organizations, etc. The dynamicity of the real world including environmental, political and social behaviors can be captured within a software agent. Also, in multi-agent systems, we have the possibility to encapsulate private data. So, we do not need additional security mechanisms to ensure data protection. One of the main characteristics of Multi-Agents Systems (MAS) is the distribution. Using MAS we can have a decentralized framework in which tasks are dispatched to agents in the system. So, we can distribute the control of data transfer and access. Therefore, we take profit from the task-delegation via agents, which is impossible with other approaches.

6 Conclusion and future work

In this paper, we proposed a new model for privacy enhancing in e-government context. This model enabled us to build an evaluative framework for trust degree reached for a given e-government process. In the context of e-government it is crucial to build a trust relationship to ensure and enforce the adoption of e-government systems by citizens. Also the proposed approach has the potential benefit of the use of only one trusted entity: the AP agent. For future works we propose to enrich our model by adding further privacy rules. We also plan to incorporate different types of risks related to privacy protection such as risks related to: data collection, data processing, data sharing, etc. Finally, we suggest managing task delegation between Admin agents to ameliorate performances of e-government systems.

Acknowledgments. This work has been supported by a common grant from Tunisian and French government relative to the project STIC DGRSRT/INRIA entitled: multi-agent coordination models for e-government systems.

References

1. Goldberg, I., Wagner, D., Brewer, E.: Privacy-Enhancing Technologies for the Internet. In: COMPCON'97, Proceedings, IEEE, pp. 103--109. IEEE Press (1997)
2. Wooldridge, M., Jennings, N.R. : Intelligent agents: Theory and practice. The Knowledge Engineering Review 10(2), 115--152 (1995)
3. Cranor, L., and al.: The Platform for Privacy Preferences1.1 (P3P1.1) Specification W3C (2004)
4. Agrawal, B., Bhattacharya, J., Gupta, S.K.: Protecting Privacy of Health Information through Privacy Broker. In: 39th International Conference on System Sciences, Proceedings (2006)
5. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. IEEE Computer 29 (2), pp. 38--47 (1996)
6. Crépin, L., Vercouter, L., Jaquenet, F., Demazeau, Y., Boissier, O.: Hippocratic multi-agent systems. In: 10th International Conference of Entreprise Information Systems, pp. 301--308 (2008)
7. Organisation for Economic Co-operation and Development: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
8. Sydenham, P.H. and Thorn, R.: Handbook of Measuring System Design. John Wiley & Sons, ISBN: 0-470-02143-8 (2005)
9. K.J. Lin, H. Lu, T. Yu, C. en Tai.: A reputation and trust management broker framework for web applications. In: IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 262--269 (2005)
10. Bellifemine, F., Bergenti, F., Caire, G., Poggi, A.: JADE- A Java Agent Development Framework. In: Multi-Agent Programming, pp. 125--147 (2005)
11. Friedman-Hill, E. : Jess The Rule Engine for the Java Platform Version 7.1p2 (2008)
12. Yang, Y., Lin, K.J., Wong, D.S. and Varadharajan, V.: Trust Management Towards Service-Oriented Applications. In: The IEEE International Conference on e-Business engineering (ICEBE 2007), pp. 129-- 146 (2007)
13. Flegel, U.: APES: Anonymity and Privacy in Electronic Services. Advances in Information Security, vol. 35, Springer US, pp. 171--176 (2007)