Privacy preservation in a decentralized calendar system

Ludivine Crépin, Yves Demazeau, Olivier Boissier and François Jacquenet

Abstract Privacy perservation, in terms of sensitive data access and management, is an important feature of decentralized calendar systems. Indeed, when users delegate their sensitive data such as timetables to an autonomous agent, this one executes many automatic data processing without their intervention: users lost a part of their data control. To tackle this problem, we propose in this article to extend a concrete application of calendars management multi-agent system by implementing a specific protocol for sensitive data transactions that represents the first step of privacy preservation in multi-agent systems.

Key words: Calendar Management, Multi-Agent system, Privacy, Sensitive Data Transaction, Interaction Protocol.

1 Introduction

In applications such as calendar management systems, users's sensitive information may be disclosed to other ones for instance while trying to schedule meeting. Considering the sensitiveness in such systems is a difficult and time consuming task. This is an even more important issue when considering

Crépin, Demazeau
Laboratoire d'Informatique de Grenoble, CNRS , Maison Jean Kuntzmann - 110 av. de la Chimie, Domaine Universitaire de Saint Martin d'Heres, 38041 Grenoble cedex 9, France e-mail: Ludivine.Crepin@imag.fr; Yves.Demazeau@imag
Boissier
Ecole Nationale Supérieure des Mines de Saint-Etienne, Centre G2I, Equipe SMA, 158 Cours Fauriel, 42000 Saint-Etienne, France e-mail: Olivier.Boissier@emse.fr
Crépin, Jacquenet
Université de Lyon, Université Jean Monnet, Laboratoire Hubert Curien, CNRS, 18 rue Benoit Lauras, 42000 Saint-Etienne, France e-mail: Francois.Jacquenet@univ-st-etienne.fr

management realized by a multi-agent system. That leads us to consider the problem of privacy preservation in terms of data management and access, like Deswarte and Melchor define it in [7].

We propose to extend a decentralized calendar multi-agent system [6] with the model of Hippocratic Multi-Agent Systems (HiMAS) [5] that takes into account this data sensitivity regarding moral issues and users' wishes.

In fact, privacy preservation must be considered during three critical steps. The first one is the storage of data that requires security. The second one is the transaction of sensitive data that requires security and many constraints in relation to users' desires (in terms of disclosure, use and retention of information for example). The last one concerns the becoming of data after a communication: we need to guarantee its protection. In this article we focus on the second critical step by implementing a specific protocol for the transaction of sensitive data [4] in a decentralized calendar application [6]. In fact, we will see that this protocol also proposes the basis for the realisation of the third step.

The next section presents the basic calendar multi-agent system [6]. Then we present the context of the extension that is the transformation of this application into a HiMAS. The fourth section defines the basis of the sensitive data protocol and the fifth section presents the implementation of this protocol into our agenda management system. We finish this article by some conclusions and some considerations for future works.

2 Decentralized calendars application

This article focuses on a concrete user-centred application presented in [6]. This application is an multi-agent approach for decentralized calendars management. The architecture (see Figure 1) proposes to represent each user by an agent in charge of the user's timetable (event scheduling, tasks, meetings).

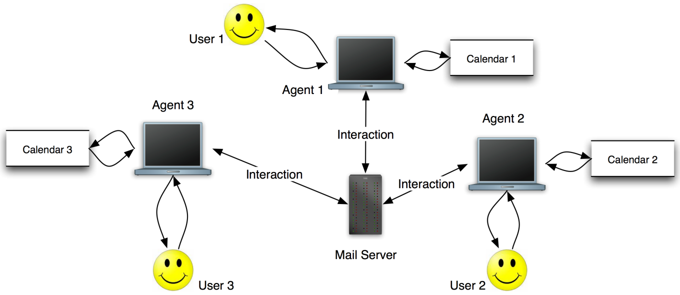

Fig. 1 Application architecture

Each timetable contains events, including tasks and meetings, that are characterized by two subjective attributes: the importance and the urgency. These attributes aim to give a priority level for each event. By default, the importance takes priority over the urgency but an agent can choose the contradictory, according to the user's wishes.

The agents in charge of the users' timetables have two possibilities to interact. The first one is the meeting negotiation based on GeNCA [8], a general negotiation API based on a contract protocol. When an user wants to fix a meeting with another user, the corresponding agent sends to the other one a proposition represented by a contract for the meeting date. The agent that receives this proposition chooses to accept or to modify this contract according to its strategy. The strategy is related to the importance and the urgency of the event and depends on the sender. Two agents that have different definition of importance and urgency do not propose same slots of times for the meeting negotiation.

The second possibility to fix a meeting is the calendars sharing. This kind of interaction is based on trust. When an agent asks another agent for its calendar, this last one chooses to send it according to its trust relationships with the first one. The trust model we implemented [6] is in direct relation with users: they determine what are the trusted agents according to their believes.

In this article, our proposition focuses only on this second kind of interaction, the calendar sharing. We propose now to introduce privacy preservation by extending this application to a Hippocratic Multi-Agent System (HiMAS) [5] presented in the next section. We consider that the sensitive data are the slots of time for each timetable, in particular the attributes of importance and urgency for each slot.

3 Foundations: Hippocratic Multi-Agent Systems

3.1 Required definitions

The **private sphere** contains data that an agent[1] considers as sensitive and all the associated management rules defining the conditions of its disclosure, its use or its sharing for example.

To represent the possible positions of an agent with respect to the private sphere, we define two roles in relation with the sensitive data transaction. The **consumer** role characterizes the agent which asks for sensitive data and uses it. The **provider** role characterizes the agent which discloses sensitive data. The provider defines a **policy** and the consumer a **preference** to define their desires regarding the sensitive data manipulations (use, disclosure...).

[1] In this approach, we consider users' as agents.

The consumer's policy and the provider's preference are defined in a similar way to the policies and the preferences defined in [12]: purpose specification, retention time and possible use. They are composed of the transaction objectives[2], the retention time of collected data, the broadcasting list and the data format (required references).

We can notice that we install a provider-centered view on the management of sensitive data, the opposite vision of the service- centered vision like for example in [9], regarding the terms of consumer and provider. This vision defines the user as the provider of information and the service as the consumer of information, it is the service and not the user that asks for data to the user and uses it. This is due to the fact that we mainly have a user-centered view on privacy preservation: users should be confident in the management of the sensitive data they delegate to their personal agent.

3.2 Nine principles for HiMAS

In order to respect the private sphere, a HiMAS must respect the nine principles inspired by the Hippocratic Databases [1] described below.

1. **Purpose specification**: The provider must know the objectives of the sensitive data transaction. Therefore it can evaluate the transaction consequences.
2. **Consent**: Each sensitive data transaction requires the provider's consent.
3. **Limited collection**: The consumer commits to cutting down to a minimum the amount of data for realizing its objectives.
4. **Limited use**: The consumer commits to only use sensitive provider's data to satisfy the objectives that it has specified and nothing more.
5. **Limited disclosure**: The consumer commits to only disclose sensitive data to reach its objectives.
6. **Limited retention**: The consumer commits to retain sensitive data only for the minimum amount of time it takes to realize its objectives.
7. **Safety**: The system must guarantee sensitive data safety during storage and transactions.
8. **Openness**: The transmitted sensitive data must remain accessible to the provider during the retention time.
9. **Compliance**: Each agent should be able to check the obedience to the previous principles.

[2] The objectives are close to the concept of goal, like for example in BDI model [2] or [10].

4 Interaction Protocol for Sensitive data sharing

4.1 Content language

For each principle of a HiMAS (and for the notion of format[3] that is required in our approach) we define an associated concept in a conceptual graph [11] (refer to Figure 2) implemented in an OWL file [13]. To formalize this conceptual graph, we use an existential positive conjunctive fragment of the first order logic in order to obtain no contradictory logical information. Each principle and the notion of format is represented by a concept linked to another according to a semantic relationship.

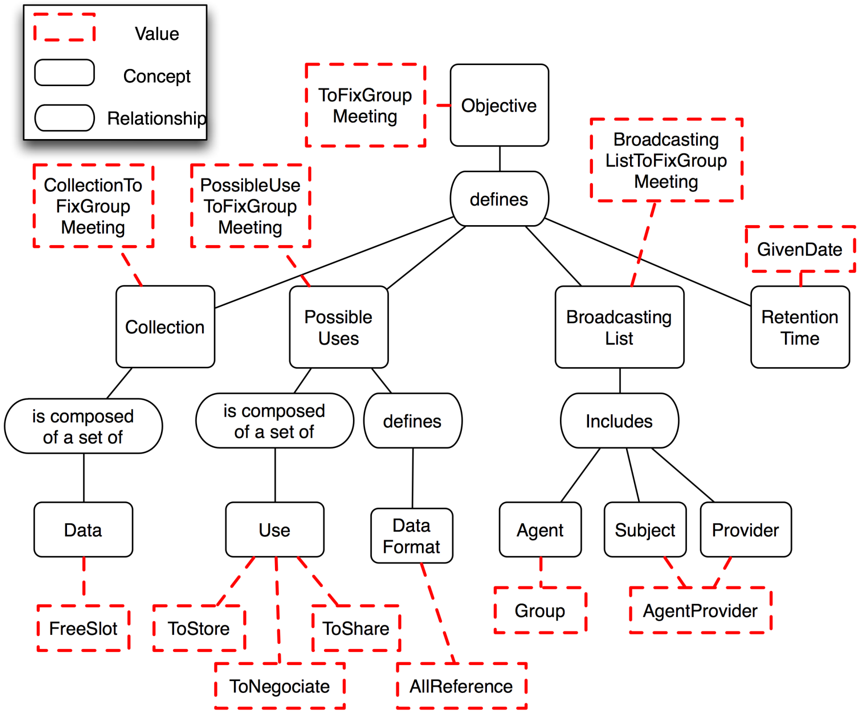

Fig. 2 Principles formalization.

To take the domain of the application into account, the conceptual graph must be instantiated by all the possible values of each concept according to the domain (refer to doted set in Figure 2).

[3] All the required references for the asked data like the urgency or the importance for instance.

To ensure the syntax, we define all the required elements of sensitive data transaction in an XSD schema. Then the HiMAS agents build an XML file that validates the XSD schema and where all the values are present in the OWL file to ensure the semantics. This system allows HiMAS agents to create sensitive data transaction with regards to privacy preservation at a semantic and syntactic level. A preference and a policy are based on the same concepts. Therefore we represent the provider's preference by the modifications that the provider induces from the consumer's policy if the policy does not match with the preference. Each consumer and each provider validate their policy and their preference using the content language in order to build and to process a sensitive data transaction with respect to the private sphere.

4.2 Sensitive data transaction protocol

We now present in a chronological order the three steps of the interaction protocol represented in Figure 3: the design of the policy, the sensitive data transaction and the design of the preference.

The first step of this protocol is the **design of the consumer's policy**. This agent builds its policy according to its objectives thanks to the content language in order to preserve privacy. Afterwards it executes the first interaction: the consumer includes its policy in a **sensitive data transaction** and sends it to the provider. The constraint of this step is that the transaction file must syntactically and semantically validate the content language (see Subsection 4.1) in order to respect agents' privacy.

Afterwards the provider begins to check the validity of the received sensitive data transaction. Then, from the management rules of its private sphere, the provider **designs its preference** thanks to the content language and tries to map this preference with the received policy. If the policy matches its preference, the provider sends the consumer the asked sensitive data. In the other way, the provider proposes some modifications to the policy in order to find an agreement. For instance, the provider can change the broadcasting list if the proposed list contains some agent that it does not trust. If the consumer accepts these adaptations, the provider sends it the data, else the consumer cancels the transaction.

This approach allows HiMAS agents to verify the constraints defined by the principles of the HiMAS thanks to the content language and so gives the basis for the compliance principle. The consumer (resp. provider) can design its policy (resp. preference) with respect to the constraints defined by HiMAS principles. This obedience is made by the semantic links between the concepts representing the HiMAS principles.

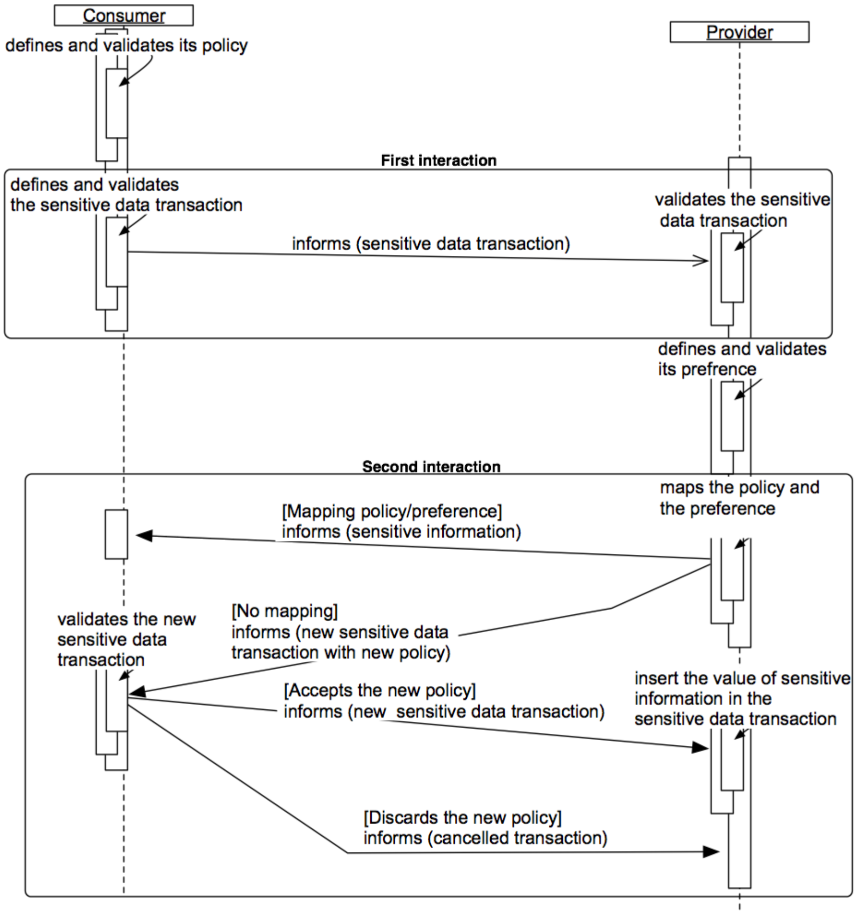
Consumer
Provider
defines and validates its policy
First interaction
defines and validates
the sensitive data transaction
validates the sensitive
data transaction
informs (sensitive data transaction)
defines and validates
its prefrence
Second interaction
maps the policy and
the preference
[Mapping policy/preference]
informs (sensitive information)
[No mapping]
informs (new sensitive data
transaction with new policy)
validates the new
sensitive data
transaction
[Accepts the new policy]
informs (new_sensitive data transaction)
insert the value of sensitive
information in the
sensitive data transaction
[Discards the new policy]
informs (cancelled transaction)

Fig. 3 Sensitive data transaction protocol

5 Implementation into the calendar application

5.1 Current implementation

In this application [6], each agent manages a calendar of one user and is registered with a specific agent, the server agent. This agent aims to deliver the message to the given agent and to prevent the agency about the subscription of a new agent. The calendar is constituted by a set of resources that represent slot of time. The negotiated contract is about these resources: each agent proposes a finite set of free resources and asks to GeNCA to find a free slot of time for each agent with regards to the importance and the urgency of the meeting. During the sharing, an agent sends to an other the asked resources.

To communicate, each message is transmitted using a GMAIL server with the Jabber protocol. This protocol allows to ensure the security, the confidentiality and the decentralization of the application.This server is represented by the server agent. At a high level, each message is defined according to a specific kind of interaction: registration, negotiation and sharing.

The graphical user interface proposes to the user one tab for each possible action: visualization of the calendar, to ask the agenda of an other user, management of the trust, informations about canceled, accomplish and current contract. The presentation of the calendar is made thanks to mig calendar that is a Java component allowing to create events visualization.

To extend this application, we propose to implement three objectives for the meeting sharing: to inform, to fix a meeting and to fix a group meeting. To give an example of our work, we present in this article only the implementation of one objective: a consumer wants to fix a group meeting with a provider and other agents (group G) in a given period of time (interval between two slots of time).

5.2 Content language interpretation

The first point of this implementation is the content language interpretation. To instantiate the classes representing the HiMAS principles, we determine the maximal set of values for each class according to the semantics relationships. For example, in order to fix a group meeting, we define the following constraints for the content language (see the doted set in Figure 2):

- The sensitive data that the consumer can collect is the free slots of time for a given period.
- The consumer can disclose this sensitive data to the group G and it must guarantee that the provider is able to access this data.
- If the sensitive data has been disclosed, all the possible references (urgency and importance) can be disclosed.
- The consumer cannot retain collected data after a given time.
- The possible uses of the collected sensitive data are storage, negotiation and sharing.

5.3 Agents reasoning

The second important point of our implementation concerns the agents reasoning. For each calendar sharing, the consumer builds its policy by parsing the content language, according to the objective chosen by the user (in the example, to fix a group meeting). The parsing of the OWL file is based on the same technique than the XML parsing. Once the consumer finds its objectives, it creates its policy in a XML file by including every possible values for each class in its policy. Afterwards this agent validates its policy: it checks that all values are present in the content language and that the XML validates the XSD file to ensure the syntax. Now the consumer can create the sensitive data transaction file, including its policy, and validates this file in the same way that the policy.

However the calendar sharing interaction is started by the user and timetables that are managed by agents represent sensitive data of users, so we need to take the user intervention into account in the implementation. Indeed, we allow users to personalize the consumer's policy. When an user wants to access another calendar, he indicates to his agent his objectives and also each policy element thanks to a form. The agent checks the validity of this policy and rejects all policy that is not valid at a syntactic and/or a semantic level. If this policy is valid, the consumer creates the sensitive data transaction and sends it to the provider. In this way, a user can choose to send an automatic or a personalized policy to the provider.

To accept the sensitive data transaction, the first condition is that the provider trusts the consumer, else the transaction is canceled. The provider begins to check the validity of the sensitive data transaction and of the policy in order to verify the consumer's intentions. If a semantic or syntactic error occurs, the provider rejects the transaction. As for the policy, the preference may then be personalized by the user thanks to a form. So, after the content language validation, the provider verifies if the received policy agrees with the user's preference. If an agreement is found, the provider sends the required sensitive data to the consumer, else the provider proposes a new policy based on the user' wishes to the consumer.

When the consumer received a new version of the policy, it accepts this one if the user has given his agreement and changed in its reasoning the terms of its policy, else the consumer cancels the sensitive data transaction.

6 Conclusion

The extension of the agenda system [6] that we propose allows users to manage their sensitive data access according to the domain of the application. To introduce this privacy preservation, we have implemented a specific protocol [4] for all the sensitive data transactions in relation to the calendar sharing interactions. Our contribution allows a dynamic management of privacy thanks to the content language and allows also users to personalize this management. Users can delegate their private sphere to the agents that respect their preferences and the private sphere thanks to the semantic and syntactic validation.

In order to ensure a complete privacy preservation in the future, we will need to implement a secure media of communication to prevent attacks. Moreover we plan to use the trust model presented in [6] to pass a judgment on the agents in relation with the past sensitive data transactions in order to prevent users from malicious behaviors. For this purpose, we need to implement the compliance principle, in particular the detection of policy violation. With this detection and the trust model, we will be able to establish a social order [3] for privacy preservation.

Acknowledgments : This work is supported by Web Intelligence project, financed by the ISLE cluster of Rhône-Alpes region.

References

1. Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippocratic databases. In *Proceedings of the International Conference Very Large Data Bases*, pages 143–154. Morgan Kaufmann, 2002.
2. Michael E. Bratman. Intention, plans, and practical reason. O'Reilly, Harvard University Press: Cambridge,MA, 1987.
3. Cristiano Castelfranchi. Engineering social order. In *Proceeding of the First International Workshop Engineering Societies in the Agent World*, volume 1972 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2000.
4. Ludivine Crépin, Yves Demazeau, Olivier Boissier, and François Jaquenet. Sensitive data transaction in hippocratic multi-agent systems. In *9th International Workshop Engineering Societies in the Agents World*, 2008.
5. Ludivine Crépin, Laurent Vercouter, François Jaquenet, Yves Demazeau, and Olivier Boissier. Hippocratic multi-agent systems. In *Proceedings of the 10th International Conference of Entreprise Information Systems*, pages 301–308, 2008.
6. Yves Demazeau, Dimitri Melaye, and Marie-Hélène Verrons. A decentralized calendar system featuring sharing, trusting and negotiating. In *Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, volume 4031 of *Lecture Notes in Computer Science*, pages 731–740. Springer, 2006.
7. Yves Deswarte and Carlos Aguilar Melchor. Current and future privacy enhancing technologies for the internet. *Annales des Télécommunications*, 61(3-4):399–417, 2006.
8. Philippe Mathieu and Marie-Hlne Verrons. A general negotiation model using xml. In *Artificial Intelligence and Simulation of Behaviour Journal*, volume 1, pages 523–542, 2005.
9. Abdelmounaam Rezgui, Mourad Ouzzani, Athman Bouguettaya, and Brahim Medjahed. Preserving privacy in web services. In Roger H. L. Chiang and Ee-Peng Lim, editors, *In Proceedings of the Workshop on Web Information and Data Management*, pages 56–62. ACM, 2002.
10. Jaime Simão Sichman and Yves Demazeau. Exploiting social reasoning to deal with agency level inconsistency. In *Proceedings of the First International Conference on Multiagent Systems*, pages 352–359. The MIT Press, 1995.
11. John F. Sowa. *Conceptual Structures: Information Processing in Mind and Machine*. Addison-Wesley, 1984.
12. W3C. Plateform for privacy preferences, http://www.w3.org/p3p/. 2002.
13. W3C. Owl web ontology language, http://www.w3.org/tr/owl-features/. 2004.