Trust and Security Enhancements in an Agent-based Workflow Management System

Noria Foukia, Bastin Tony Roy Savarimuthu, Maryam Purvis, Yanhua Han

University of Otago, P O Box 56
Dunedin, New Zealand
{nfoukia, TonyR, Tehrany, yhan}@infoscience.otago.ac.nz

Abstract. This paper describes the trust and security features that are integrated in an agent-based Workflow Management System. In a workflow scenario, information is passed from one participant to another and may be accessible by different interacting enterprises involved. In this environment trust is an important issue to be established between various collaborative entities. The level of trust is computed based on the past and the current performance and other relevant parameters. We explain how the workflow manager specifies the parameters associated with the calculation of trust. In addition, our paper addresses access control issues in terms of authentication and authorization to access various services offered for different types of users interacting with the Workflow Management Systems (WfMS). This paper also explains how the users of the WfMS can specify their privacy preferences and how privacy policies are used during the enactment of a business process.

1 Introduction

Workflow Management Systems (WfMS) are used to manage business processes associated with distributed global enterprises [10]. These business processes are managed by workflow systems that support interaction between enterprises. Each enterprise has certain resources and offers certain services. When combining distributed resources and services among different enterprises, which are often located in different administrative domains, the WfMS should ensure that [7]:

1. The services and resources are provided in accordance to the criteria specifiedto the user.
2. The information provided by the interacting entities is not misused.

Trust is a notion suitable for a WfMS managing workflows in a distributed and open environment because:

- IIn an open environment a WfMS makes use of external actors (services, customer) whose trustworthiness is not known in advance.
- Trust is a dynamic entity that evolves as participants interact which each other over time. It is computed based on past and current behavior of the users.
- Interactions and collaboration between resources/services are possible if an acceptable level of trust is established between enterprises. Trust helps the enterprises to decide if they want to collaborate. Moreover, sensitive information can be exchanged and stored during the business processes managed by a WfMS. WfMS should provide mechanisms to secure the exchange and the use of sensitive information. This could be provided by encrypting data, signing data, defin-

ing roles and assigning privileges, etc. However, even with these mechanisms two parties involved in a business process may be reluctant to reveal personal or sensitive information. By establishing an acceptable level of trust, they could accept the risk to disclose sensitive information. But, in the particular case of open workflow system, information could leak out of one enterprise during business interactions. Therefore, the WfMS must also provide adequate control and protection to guaranty any sensitive information routed during the business process. At each step of the workflow process, the WfMS must support access control policies that regulate access to resources and services, and privacy policies that regulate the conditions of disclosure and use of sensitive information during the workflow process.

This paper introduces security and trust features that are added to our existing WfMS outlined and implemented in [12][13]. Figure 1 describes the prototype WfMS which is made up of a number of agents who are responsible for various tasks associated with the WfMS. The workflow manager agent provides the interface to the workflow administrator who can select an appropriate process model. Through this interface, various resources are made available to the system for the execution of different tasks within the model. The process agent is responsible for the execution of the process model. The resource broker agent provides the interface to various workers (resources) involved in performing the tasks specified in the process model. The monitoring and controlling agent are responsible for recording various data associated with the performance of the system in terms of processing of the work-cases[1] and looking for pre-determined set of anomalies which may require the system administrator's attention or intervention.

The tasks specified in the process model are either automated such as looking up a particular entity in the database (to ensure whether a product exists in the warehouse) or they need a human intervention such as documents that need to be signed by a designated human resource. As a part of the automated tasks, the service could be either internally available (i.e. printing a set of forms using the printer device owned by the organization) or externally available (login to an external database in order to obtain the credit information for a particular customer). In the implementation of our current prototype some of these external services are provided through known Web services which the workflow administrator has registered in advance. However, in our open system, we also allow dynamic discovery of services as well as invocation of specific operations offered by these services when appropriate.

In our prototype WfMS, there are different types of users with different concerns and expectations from the system:

- The workflow administrator is responsible for the overall operations of the system (creating the process models, allocating resources[2] (workers) and monitoring the status of the system).

[1] Work-case is an instance of a particular job during workflow enactment. A WfMS can have a large number of work-cases at any point of time, each representing a particular job.

[2] In a WfMS the resources can be classified into human-resources and non-human resources(printers, scanners) etc. In this paper we refer to human-resources (workers).

- The workflow workers (resources) are responsible for registering themselves with the system and they specify their availability for performing a task. The workflow workers may specify one or more roles that they can fulfill. In addition, they should be able to check the status of the system in order to help the customers with a specific enquiry in terms of the status of the processing of a particular request.
- The workflow customer can access the system to send a request to the WfMS. Request submission scenario is presented in Figure 1.

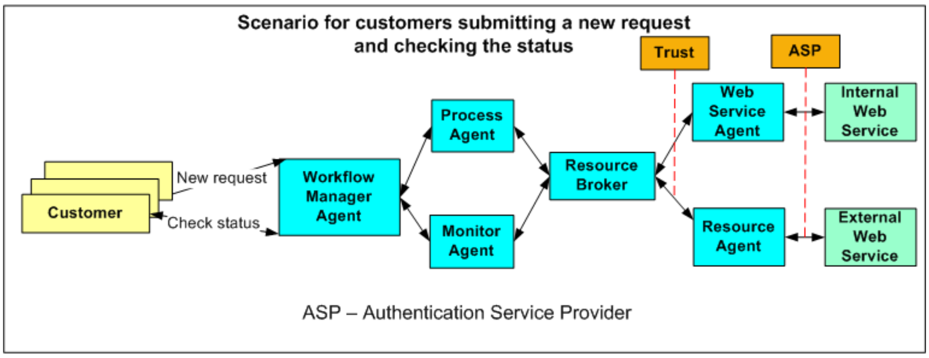

Figure 1: Scenario that describes the submission of requests from a customer

The WfMS prototype presented in [12][13] lacked security features such as authentication module that is flexible, distributed, and adaptable. This paper introduces the enhancements that are made to the system by adding the following components
(a) A security module: This module is composed of 3 different components, namely the Authentication Service Provider (ASP), the Access Controller (AC) and Single-Sign-On (SSO) service. Authentication and authorization of various services offered for different types of users interacting with the WfMS are provided respectively by the ASP and the AC.
(b) A trust module : The trust module computes the level of trust associated with a particular entity. The entities associated with the WfMS include customers, workers and service providers. The parameters associated with the calculation of the trust is specified by the workflow manager.
(c) A privacy repository : The paper also explains how privacy policies are can be created and used in the workflow process.

2 Related Work

Agent based workflow management system is an active area of research. In our earlier works we have described the work done by other researchers in this field [13, 14] The scope of this section is to relate to the work that has been carried out in the areas of privacy, security and trust in the context of WfMSs.

Workflow management systems are utilized by a wide range of business enterprises and the need for security, privacy and trust has been acknowledged in the research community [3,4,5,6,7]. Security specifications for WfMSs has been proposed by WfMC [8]. The WfMC does not address privacy and trust issues for workflows. There has been some extended work on security for WfMS [9], which explain the security issues using examples. But this work does not incorporate trust issues, which are central to a distributed workflow environment.

Using agents to build WfMSs calls for addressing privacy and trust issues. Lack of standards for secure multi-agent systems has given rise to the multitude of implementations. Foundation of Intelligent Physical Agents (FIPA) [1] security specifications is limited in providing specific guidelines for addressing trust issues. Many researchers have worked on making agent interactions secure [2,3,4] by introducing authorization and authentication mechanisms. Some researchers [5,6,7] have focussed on notion of trust-based model for agent based communication and negotiation.

Workflow presents interesting scenarios in which trust plays an important role in areas such as resource allocation as clients, workflow managers and workers and services can be entangled in a web of deception. Privacy is also a concern in most workflows as the personal data of the customers/workers involved in the process might be at jeopardy (ex. Health workflows, Banking workflows).To our knowledge there has been limited work on trust and privacy issues related to WfMSs. So, in this work we describe how we incorporate modules in a workflow system that can compute the trustworthiness of the resources and services involved and modules that incorporate secure access to the system and protect the privacy of the personal data associated with the consumers.

3 Security Enhancements

3.1 Addressing Privacy and Trust in the WfMS

In this subsection, we describe how the concept of trust is applied in WfMS.

At the task execution level the resource broker determines an appropriate worker. Initially, the resource broker identifies a list of resources that are capable of performing a particular task based on the roles specified for each worker. Then, it consults the trust agent and identifies the best resource based on the trust level associated with that resource.

During the execution of the WfMS , different parameters will be considered to allow for appropriate security and trust concerns associated with various entities involved. These parameters are listed below:

- **The current System Status (SS)**:

For example, the load of the WfMS maybe one of the contributing attributes in determining the SS value. Based on the current SS value, the accepted trust threshold is adjusted. For instance, if the load of the system is heavy, we may be more tolerant in selecting a particular resource.

- **The suspicion level (SL) associated with the customer, worker, and service:**

For example, before an external service is used, the trust (SL value) associated with that entity is calculated. This SL is computed based on the customer's history (past transactions and behavior stored in her history file). An example of the set of parameters associated with each entity is given in section 4.

Trust calculation for the resources in the WfMS:

In our current system, the trust value associated with a resource is directly related to the resource's past performance, reliability, and how he has been assessed by others (i.e. peer workers, customers). Note that these parameters can be dynamically specified by the WfMS manager depending on the nature of the business process and associated interacting entities. Each of these attributes is attributed to a sl_i and has a weight (w_i). These values are specified by the workflow manager which reflect the value associated with a particular parameter for an entity and its importance from the point of view of the manager. For instance, if the parameter i which represents reliability of a worker, has a high suspicion level (sl_i), that means that the worker is not reliable. If the corresponding weight associated with reliability is 1.0, that means that the workflow manager considers reliability to be an important factor in trust calculation.

In the WfMS, trust (T) is computed by the formula:

$$T = 1 - \frac{\sum_{1 \le i \le n} w_i \times sl_i}{\sum_{1 \le i \le n} w_i} \qquad \textit{(Formula a)}$$

where n is the number of parameters specified by the workflow manager. In our case we have n=3 for the three main parameters that are specified in the example given in Table 1.

Attributes	**Suspicion Level (sl_i) (0.0 – 1.0)**	**Weights (w_i) (0.0 – 1.0)**
Performance	0.9	1.0
Reliability	0.7	0.5
Peer Assessment	0.8	0.8

Table 1: Worker's attributes for trust determination.

Table 1 shows the attributes and corresponding weights and suspicion levels for a particular worker. The weights are determined by the From a manager's viewpoint performance could be the most important factor followed by the peer assessment. The suspicion levels for performance and reliability are calculated based on the manager's assessment of the worker and the peer assessment is based on the peer reviews obtained from the colleagues, sub-ordinates of the worker under assessment.

Developing trust with external services:

For external services the attributes associated with calculating the trust depend on the characteristics of a service that may be consider important. For instance, in the WfMS the attributes associated with a web service may include availability of the service, quality of service, and performance of the service etc. T is calculated in the same way as shown by *formula a*.

In this subsection we describe how the privacy policies and preferences are applied in the WfMS.

For the reasons mentioned in the section 1.1, the WfMS requires that the information passes from one participant to another and is stored at the appropriate location, but, it also requires that the particular worker and/or service has the appropriate right of access to the information. This information is often related to people and their activities and can be classified as sensitive or personal data. Therefore, in the workflow process, privacy concerns are raised. While data capture is often critical for the correct functioning of governments, public services and business, it may also facilitate unobtrusive access, manipulation and presentation of personal data [11].

To protect sensitive data in a WfMS with interacting enterprises which might have different privacy preferences and interests, privacy policy preferences are negotiated with the WfMgr Agent and a policy enforcer module (Policy Agent) is used.

During the execution of the workflow, the federated institutions can have some interactions with each other in the form of requesting some service from each other such as an insurance provider may ask for some patient information from the health service provider. In this situation, privacy policy statements are first checked before any information is exchanged from one provider to the other. These policies are specified in the registration phase through an informal negotiation process where the customer specifies her privacy preferences to the WfMgr Agent. If the WfMgr Agent cannot accept the proposed request by the customer, through negotiation, either a compromised position is achieved or further negotiation is stopped. For instance, this situation can happen if the customer registers for a service and her privacy preferences contradict the privacy policies already negotiated between the WfMgr Agent and the service provider. These inconsistencies are checked by the Policy Agent at the registration phase. When a negotiation succeeds, the agreed policies associated with the negotiation are generated and stored in the privacy policies of the corresponding actor and the privacy preferences are registered in the actor's profile. The new generated privacy policies agreed between the WfMS and the customer integrate the policy preferences that do not contradict existing privacy policies related to the usage of the workflow system by the customer. The existing policies are:

- Internal policies negotiated with workers or associated to internal services.

- External policies negotiated with other customers or associated to external services.

During the workflow process inconsistencies may happen that were not detected at the registration phase. For instance, if a requested service is not available anymore, the Resource Broker can offer an equivalent service. In this case, the customer may be asked to relax her preferences before using the service.
Figure 5 (top) shows the privacy preference negotiation during the registration phase and also (bottom) the privacy relaxation during a workflow process when a service is requested by a customer.

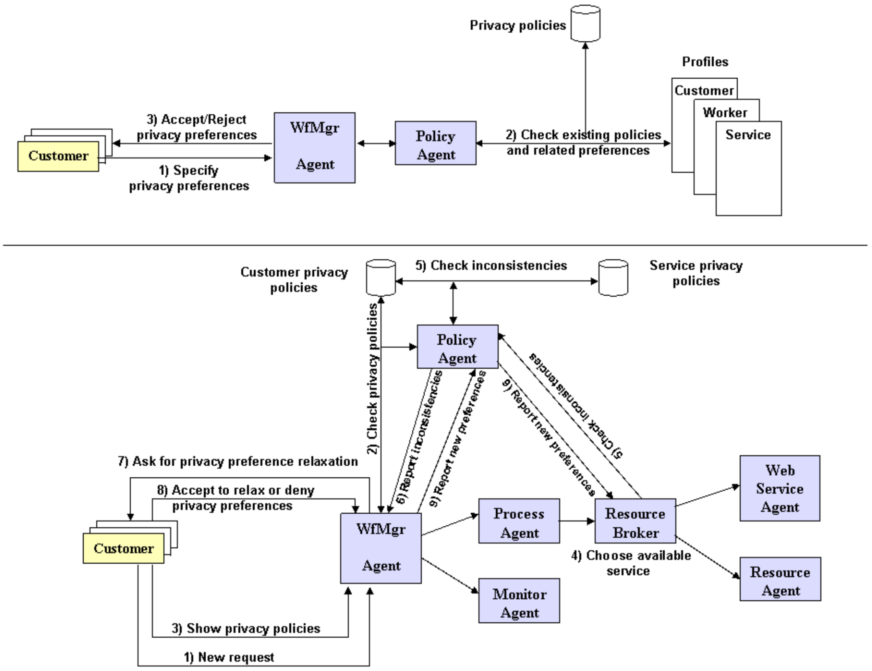
Privacy policies
Profiles
Customer
Worker
Service
3) Accept/Reject privacy preferences
Customer
WfMgr Agent
Policy Agent
2) Check existing policies and related preferences
1) Specify privacy preferences
Customer privacy policies
5) Check inconsistencies
Service privacy policies
Policy Agent
2) Check privacy policies
6) Report inconsistencies
9) Report new preferences
6) Report new preferences
5) Check inconsistencies
7) Ask for privacy preference relaxation
8) Accept to relax or deny privacy preferences
Customer
WfMgr Agent
Process Agent
Resource Broker
Web Service Agent
4) Choose available service
Resource Agent
Monitor Agent
3) Show privacy policies
1) New request

Figure 5: Privacy preference specification (top) and dynamic privacy relaxation(bottom)

3.2 Addressing Access Control and Authentication in the WfMS

3.2.1 Use of ASP to Secure the Authentication in the WfMS

The WfMS incorporates a new security module composed of 3 components, namely the Authentication Service Provider (ASP), Access Controller (AC) and Single-Sign-

On (SSO) to ensure proper security and determine the appropriate level of access and privileges to various services. This module provides the following functionalities.

1. **Authentication service**: the system can only provide service for approved users. So any user must enter username/password to verify her legal status. The system makes sure that the password is irreversibly encrypted using SHA algorithm and SSL for secure password transfer across networks.
2. **Access control via the AC**: different users (customers, administrators) can access different functions and data. Access control specifies what action a role can take and what information can be accessed depending on the role(s) played by each user.
3. **SSO service when accessing the web service:** to make it easy for the user. ASP provides SSO function when accessing internal web service.

Figure 6 shows the steps involved while authenticating a user which is carried out by the Authentication Service Provider (ASP) module. When the WfMS needs to access Web services it uses the SSO mechanism, which enables the user to access a particular service.

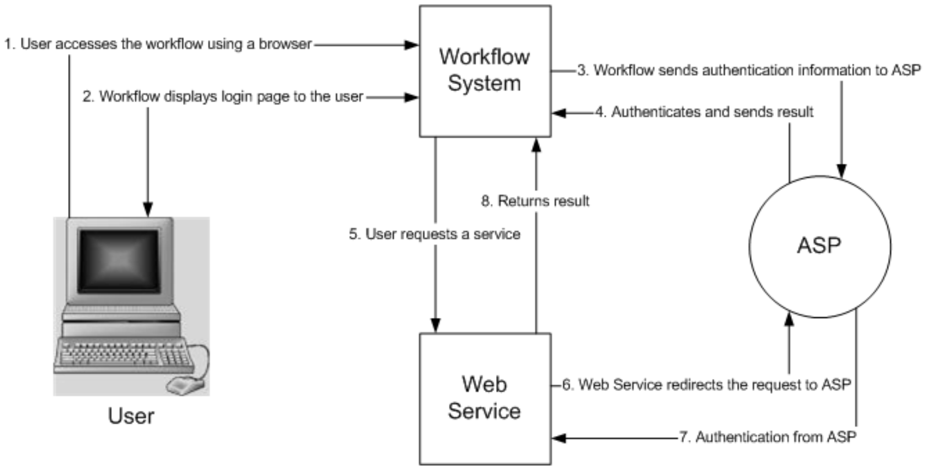
1. User accesses the workflow using a browser
2. Workflow displays login page to the user
Workflow System
3. Workflow sends authentication information to ASP
4. Authenticates and sends result
8. Returns result
5. User requests a service
ASP
User
Web Service
6. Web Service redirects the request to ASP
7. Authentication from ASP

Figure 6: The Authentication Process of SSO by ASP

In this scenario we are assuming that the web service is part of the federated service providers.

4 Scenario-based Demonstration

In this section, we present different security related scenarios that would arise in the context of WfMS. There are two stages of handling security, namely, the registration stage and the workflow enactment stage.

4.1 Registration Stage

Initially the workflow manager configures different parameters in the system which are:

1. The description of the roles and tasks
2. The description of resources and their assigned roles
3. Definition of the parameters involved in the computation of trust and their respective weight. Default values are assigned to each parameter.

During the registration phase, customers (external entity) or workers (internal entity) will register to the WfMS.

- A customer can register to a simple service which requires no authentication via the ASP module of the WfMS. An example is when a customer accesses a list of books in an on-line library. Or a customer can register to a service which requires authentication via the ASP module (for instance, for banking service). In this case the WfMgr agent delegates the authentication process to the ASP module.

- For a new worker, the registration procedure depends essentially on the initial parameters associated with the worker as specified by the WfMS administrator. Each worker is attributed default roles, a name and a specific identifier (id) as well as a default access password (can be changed after initial log in). When a worker logs in to the WfMS for the first time, she will be presented an initial login session by the WfMgr agent. During the login session, the worker will have to provide her name/id/password to enter the workflow system. She will only have access to the default resources and services associated with her roles. However, after she logs in, she may ask the WfMgr agent to assign a new role so that she can access a resource not listed in her default profile/parameters.

4.2 Workflow Enactment Scenario

To illustrate the concepts introduced in the previous section, we describe a car insurance scenario. Suppose that the WfMS belongs to the insurance company and that a customer (C) of the insurance company damaged her car in a car accident. We assume that this particular car was made by MAKEC company. Then, via the WfMS, C contacts the secretary (worker S) of the insurance company. To process any request from C, S asks first C to provide her insurance policy number. After validating C's policy number, S transfers the request (workflow) to the car insurance company expert (worker E). E asks C to provide a detailed description of the damage caused to her car (via an on-line form). After C fills the form, E will choose an appropriate mechanic (service provider M) to send the car so that it can be repaired. Then, E consults the insurance company WfMgr for final approval and then notifies C of the outcome.

In this scenario several cases could happen that will use the concepts described in section 2:

1. The System Status (SS): Suppose that the customer has specified in his preferences that he would prefer an expert of the MAKEC. Suppose that all workers with a good expertise in MAKEC are not available, then the WfMgr could decide to assign a worker with less expertise in MAKEC. For the WfMgr the important criteria is to increase the customer satisfaction by decreasing the time he is waiting for his car to be fixed. The level of expertise is based on the trust T attributed to the worker. A worker with a good performance and good reliability in his past work experience and who received good feedback from his colleagues and customers will be attributed a higher level of trust.
2. Level of trust (T) and the SL=<sl_i> (sl_i between 0.0 and 1.0)

   Suppose that C already had a previous car accident and that the previous car was already sent to the same mechanic M. Suppose that C was not happy with the service provided by M for two reasons:

   - In case 1), M took a long time to repair the car (more than what was estimated at the beginning).
   - In case 2), when M changed the bumper, the bumper did not last for more than 3 months.

   In this situation when the worker presents the choice (M) to C, C may decide to refuse the mechanic and ask for another one in the list of the mechanics provided by the worker. In the situation of a refusal, the WfMgr can ask the customer to specify the reasons of the refusal. C will send her feedback to the WfMgr:

   - In case 1), the trust module will increase the suspicion related to availability $\mathbf{sl_1}$ by 0.1**.**
   - In case 2), the trust module will increase the suspicion related to the quality of service $\mathbf{sl_2}$ by 0.1.

   The suspicion level attributed to the performance $\mathbf{sl_3}$ will not change because M maintains the same car repair rate per day. Table 2 gives an example of the previous values attributed to $\mathbf{sl_i}$ and the corresponding weights w_i. The WfMC administrator attributes a higher importance to quality of the service and the performance provided by the M than availability. Formula b computes the new corresponding T.

Attributes	**Previous sl_i (0.0 – 1.0)**	**w_i (0.0 – 1.0)**	**New sl_i (0.0 – 1.0)**
Availability	0.7	0.5	0.8
QoS	0.7	1.0	0.8
Performance	0.5	1.0	0.5

Table 2: Mechanic's attributes for trust determination

$$T = 1 - \frac{0.5 \times 0.8 + 1 \times 0.8 + 1 \times 0.5}{0.5 + 1 + 1} = 0.32 \qquad \textit{(Formula b)}$$

As the new T attributed to M increases the WfMS will check if this new value will validate any control policy condition and if that any action should be taken. One policy could be that if T ≤ 0.4 do not offer the service to the customer for a certain period of time. Applying a penalty is a means for the WfMS to express its disagreement with the service provided by M and to give M incentives to take his responsibility for the bad service provided as a consequence on the customer's distrust.

3. Privacy policies and preferences

Suppose that the car insurance is federated with a health insurance which is C's health insurance. Suppose that the C has specified in his preferences that he must be asked for an agreement before any information is disclosed to federated institutions whose list was presented to him at the registration stage. During the car accident, C was physically injured and he also made a request to his health insurance to be refunded for the expenses caused by the medical care apart from applying for car insurance. The request is handled by a WfMS of the health insurance and a worker (W) of the health insurance sends a request to receive the accident report from the car insurance. When receiving the request WfMgr agent of the car insurance will first check the privacy policies agreed with C during the registration phase. Since C requires to be contacted before any information is disclosed, WfMgr agent asks C first for his agreement. If C accepts then the request made by W is processed, otherwise W is notified that due to privacy protection, such information cannot be disclosed. If the information cannot be disclosed it could have an influence on the trust made by the health insurance.

5 Conclusion and Future Works

In this paper we have described security enhancements that make the WfMS more secure. These enhancements allow for a mechanism that dynamically calculates trust values associated with various entities involved. In addition the paper also describes the security and privacy issues associated with inter and intra organizational activities that involve sensitive data. The system also allows for flexible choices of resource allocations and services when an acceptable level of trust is reached. We provide a new mechanism by which the user of the system can dynamically change her privacy preferences at any time of the workflow enactment, particularly in conflicting situations. This is beneficial because this improves the trustworthiness of the WfMS.

In future we are planning to incorporate formal negotiation mechanism during the selection of a particular service and also when the WfMS offers different services.

References

1. Joint Submission, FIPA Specification. Accessed at http://www.fipa.org, 1997
2. Zhang, M., Karmouch, A.: Adding Security Features to FIPA Agent Platforms. 2001, http://www2.elec.qmul.ac.uk/~stefan/fipa-security/rfi-responses/Karmouch-FIPA-Security-Journal.pdf, Accessed on 20th January 2006
3. Wen, W., and Mizoguchi, F.: An Authorization-Based Trust Model for Multiagent Systems. Applied Artificial Intelligence (2000) 909-925
4. Yuh-Jong, H.: Some Thoughts on Agent Trust and Delegation. Proceedings of the fifth international conference on Autonomous agents (2001), Montreal, Quebec, Canada, 489-496
5. Maximilien, E.M., Singh, M.P, Agent-Based Trust Model Involving Multiple Qualities. Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2005)
6. Casassa, M., Mont, M., Crane, S., Pearson, S., Handling Privacy Obligations and Constraints to Underpin Trust and Assurance. Hewlett Packard reference number: HPL-2005-54 20050318
7. Ryutov, T., Zhou, L., Neuman, C., Foukia, N., Leithead, T, Seamons, K.E., Adaptive Trust Negotiation and Access Control for Grids. 6th IEEE/ACM International Workshop on Grid Computing, Seattle (2005)
8. FIPA Security Specifications. Accessed at http://www.wfmc.org/standards/docs/TC1019_10_SecurityPaper_1998.pdf
9. Atluri, V., Security for Workflow Systems. Accessed at cimic.rutgers.edu/~atluri/workflow.pdf, Accessed on 25th January 2006
10. Van der Aalst, W.M.P., Van Hee , K., Workflow Management: Models, Methods and Systems, MIT Press 2002
11. Kling, R., Dunlop, C., Computerization and Controversy : Value Conflicts and Social Choices. San Diego: Academic Press, 1991.
12. Savarimuthu, B.T.R., Purvis, M.A., Purvis, M.K., Cranefield, S.: Integrating Web Services with Agent Based Workflow Management System (WfMS). Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence (WI 2005), ISBN 0-7695-2415-X, IEEE Press, Los Alamitos, CA (2005) 471-474
13. Ehrler, L., Fleurke, M., Purvis, M. A., Savarimuthu, B.T.R.: Agent-Based Workflow Management Systems (WfMSs): JBees - A Distributed and Adaptive WFMS with Monitoring and Controlling Capabilities. Journal of Information Systems and e-Business, ISSN: 1617-9846, Journal no. 10257, Volume 4, Springer, Berlin (2005), 5-2214.
14. Savarimuthu, B.T.R., Purvis, M. A. and Fleurke, M. (2004), Monitoring and Controlling of a Multi-agent Based Workflow System, Proceedings of the Australasian Workshop on Data Mining and Web Intelligence (DMWI2004), Conferences in Research and Practice in Information Technology, Vol. 32, Australian Computer Society, Bedford Park, Australia (2004) 127-132.