# Towards an Ontology-based Organizational Risk Assessment in Collaborative Environments Using the SemanticLIFE

Mansoor Ahmed, Amin Anjomshoaa, Tho Manh Nguyen, and A Min Tjoa
Institute of Software Technology & Interactive Systems,
Vienna University of Technology,
Favoritenstrasse 9-11,
1040 Vienna, Austria
E-mail: {mansoor, anjomshoaa, tho, amin}@ifs.tuwien.ac.at

***Abstract*— The rise in interconnectivity in the last few years has made computer systems and networks more vulnerable to threats as they are accessed by an ever increasing number of users. Nowadays organizations are lacking proper security measures and means to calculate risk assessment for their assets. Legacy systems in organizations are facing different kind of risks like viruses, bugs and system failure causing damages to hardware and software resulting lost of data.**

**The ultimate challenge in many organizations is to assess their risk factors for their computers and networks. There is no way to completely overcome the threat that an organization might have. The goal is to calculate risks, so that problems resulting from them can be minimized and to fill the gap between business entities (like a project, a role) and organization infrastructure using Semantic Web technologies. SemanticLIFE is a Personal Information Management System which gathers the user interaction events and correlates those using ontologies. In this paper we will explore ontology-based risk assessment method using SemanticLIFE tool for organizations security which is a fundamental issue for planners and decision makers in IT field.**

## I. Introduction

The wide spread use of the Internet and Information advanced technologies in the variant application domains results in the ubiquitous data distribution amongst different computing systems. People nowadays do not only work or access data on their own computing system, but they also need to work in other systems within the collaborative environment. The need for safe and secure systems that are capable of sharing the data securely, detecting the risks, preventing attacks, reducing the vulnerable effects and so on becomes more and more essential, especially in collaborative environment.

Attacks could come in various ways depending on the environment in which the systems were deployed and the data they process. The users non-authorized accesses to data, illegal packages execution, virus distribution, spam emails, server hacking, are some of examples of attacks that could happen every day. Each attack has different levels of danger and effects on the systems. Some attacks could be very dangerous, and affect the whole organization, while some limit only to the personal computer. Detecting and preventing attacks are time and budget consuming task in administration of an IT-organization. The system administrators should track the changes in heterogeyneous running systems with different installed software, operating systems, processes and applications.

Beyond all the complexities mentioned above, the system administrators should take care of the side effects of the combination of software and hardware configurations that might put the computers and network at risk. On the other hand this data should be merged with other business aspects of an organization, like business processes, projects, tasks, roles, etc. Usually the system administrators are not that much aware of business concepts and are more equipped with pure technical skills. As a result there is usually a gap between organizations' business entities and the software, hardware and human resources. The Semantic Web technologies seem to be a good candidate to bridge this gap and assist the system administrators to manage and control the systems more smartly. On the other hand a semantic combination of entities-resources will enable the administrators and managers to minimize the side effects of their decisions that might put the organization at the risk.

Another major challenge is the information gathering about the physical entities (i.e. mail servers, web servers, databases, personal computers) and the softwares, applications installed on them. Such informations changes dynamically time by time and is also scattered in the organization. The relation between those entities (i.e. which computer/server belongs to the people from the same project, which process could cause domino effect if being stopped or killed due to its belonging to several entities, etc) should also be managed so that the suitable security policy could be issued within the organization. Closing the gap between physical entity information, the objects running, and semantic information of dependency relations between them to asset the attack risks are the purpose of our approach using SemanticLIFE in organizational risk assessment.

This paper is organized as follows. In Section 2, we review related work. In Section 3, we discuss the overview of security and privacy concepts in semantic web, section 4 contains

SemanticLIFE architecture, section 5 consists of problem statement and usecase scenario, section 6 describes the use of ontologies, section 7 propose solution and section 8 shows our ontology-based risk assessment approach, in section 9 we discuss the conclusion and the future work.

## II. Related Works

Risk assessment in Information Technology has been deeply investigated in [1]. This is a guideline of risk classification and risk evaluation in the general domain of Information Technology System. The authors also state that reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing. They propose some case studies on risk assessment methodology in various companies.

The author in [2] suggests a methodology which could extract, model and analyze the security requirements from multiple documents and then use the ontological process to infer valuable knowledge on system secure assurance. The approach, however, could only be possible in case already existing the well-established Certification and Accreditation (C&A) documents.

Ontologies have been applied in the security management domain to overcome the complexity of modern information systems [3], [4]. A number of security-related knowledge sources within organization are kept in the security ontology which is the centric of the security framework. The specific Risk Assessment security ontology [5] was built to manage the security requirement and the threat countermeasure assessment. The proposed ontology describes in details of variety of threats and the association between the threats and the countermeasures although the threat asset measurement is quite simple. [6] presents an approach to corporate assets in a company when taking into account the entire infrastructure. The approach proposes a quick calculation of effective countermeasures using the security ontologies. The company infrastructures such as computer, network, server, person, etc are taken into account in measurement evaluation. However, the model uses some heuristic estimation parameters thus could cause imprecise risk evaluation results. Our paper will go a step further by suggesting more precise risk assessment model which also take into account the semantic relation between the business objects.

Ontologies are also widely used in other specific security sub-domains such as network security [7], data privacy [8], access control [9], [10], pervasive computing [11], [10]. However, the existing researches do not consider the affection of threats in the entire enterprise which is one of our papers aims.

## III. Overview of Security and Privacy in Semantic Web

The World Wide Web (WWW) is a huge information source with nearly enormous potential. The current web technology cannot be processed by machines and presented in a better and meaningful way. Also the information which is available on the web cannot be fully utilized and accessed because of weak publishing. Semantic Web is an effort to bring meaning into web pages contents. Semantic Web is not a separate web, its an extension of the current web where bulk of information is linked up in such a way that they can be easily processed by machines and can be presented in a meaningful way. Thus with Semantic Web, when a user searches for some information, he/she gets results which are not only precise but also relevant and according to his/her preferences. [12].

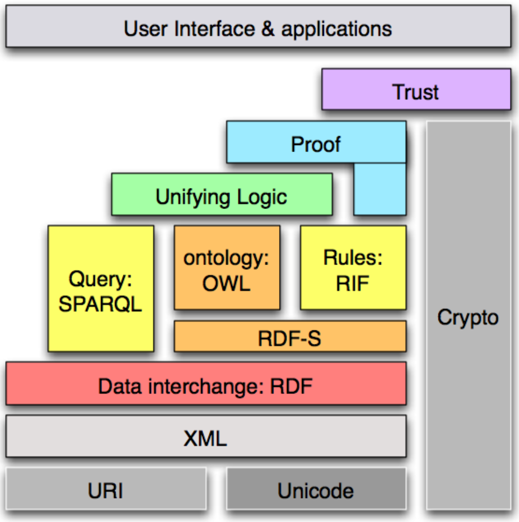

Fig. 1. Semantic Web Architecture by W3C

Tim Berners Lee has specified different layers for semantic web as depicted in Figure-1. The top layer in the semantic web cake is trust and proof. But security cut across all the layers [13] .In past few years there has been lot of development on semantic web [14]. It is essential that semantic web should be secure, which means that its components like XML, RDF and ontologies should be secure.

The rapid growth in information systems has resulted in computerizing applications in various domains. Individuals can store nearly every kind of digital information in their systems. In organizations where data plays an important role it has become easier to share information. The organizations with project development environment, it is useful if there is possibility of sharing information among different project members and access to data.

While discussing security issues on semantic web, one should not forget the importance of privacy. Privacy means making some part of your document public while keeping others as private. Privacy issues have gained a lot of attention recently especially in the area of personal information management. Privacy plays an important role in situations where agents will be interacting with each other for the retrieval of information. Privacy can be maintained effectively by making use of the semantic web technologies. In contrast to existing web the semantic web allows to describe resources in the form

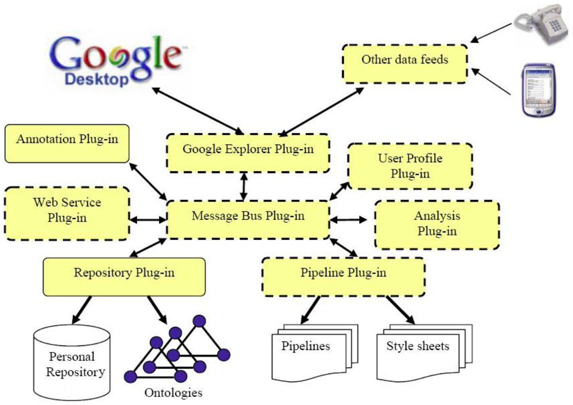

Fig. 2. SemanticLIFE Framework Architecture

of triples where group of triples could be annotated as public or private. [15] presents convincing examples of ontology based privacy management. For example *Alex* published his resume as an RDF document and annotated that certain fields, such as phone number and postal address, should not be disclosed. Now when a *recruiting agent* comes across that resume the only parts which are declared public by *Alex* will be shown.

Nowadays' best practiced way on the web for describing privacy policies is P3P which uses XML to describe policies in machine-readable format [16].

## IV. SemanticLIFE Architecture

The SemanticLIFE framework is developed on a highly modular architecture that provides the basic components for the proposed collaboration mechanism that will be discussed in later sections. SemanticLIFE stores, manages and retrieves the lifetime's information entities of individuals. It enables the acquisition and storage of data while giving annotations to emails, browsed web pages, phone calls, images, contacts, life events and other resources. It also provides intuitive and effective search mechanism based on the stored semantics.

An overview of the system architecture is depicted in Figure 2. The whole SemanticLIFE system has been designed as a set of interactive plug-ins that fit into the main application and this guarantees flexibility and extensibility of the SemanticLIFE platform. Communication within the system is based on a service-oriented design with the advantage of its loosely coupled characteristics. To compose complex solutions and scenarios from atomic services from SemanticLIFE plug-ins, the Service Oriented Pipeline Architecture[1] (SOPA) has been introduced. SOPA provides a paradigm to describe the system-wide service compositions and also external web services as pipelines. SOPA provides some mechanisms for orchestration of services and transformation of results. Due to the significant role that this component plays in the proposed solution, it will be explored in more details in the next sections.

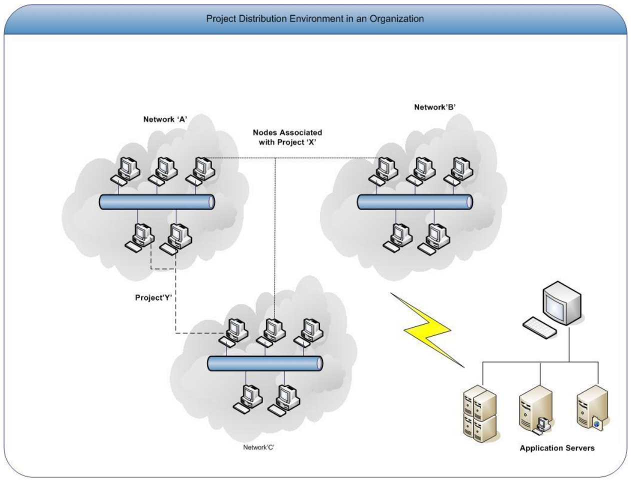
Project Distribution Environment in an Organization
Network 'A'
Nodes Associated with Project 'X'
Network'B'
Project'Y'
Network'C'
Application Servers

Fig. 3. Project Distribution to Nodes

Data with user annotation is fed into the system using a number of dedicated plug-ins from variety of data sources like Google Desktop2 captured data, communication logs, and other application's metadata. The data objects are passed on by the message handler to the analysis plug-in. This plug-in contains a number of specific analysis plug-ins providing semantic mark-up by applying a bunch of feature extraction methods and indexing techniques in a cascaded manner. The semi-structured and semantically enriched information objects are forwarded to the repository plug-in for an ontologically structured storage, so called the meta-store. A set of query processing and information visualization tools provides the means for information exploration and report generation. The analysis module and metadata extraction capabilities make associations among the lifetime items and lifetime events based on user annotation, user profile and the system ontologies.

## V. Problem Statement and Use Cases

Consider a project development environment in an organization, where different people like programmers, developers, quality assurance and architects are working on different projects distributed on different nodes. Organizations with such setup usually work in distributed environment, that means project is distributed on different nodes like database server running at one node while application server, versioning system like (CVS, SVN) and web server at some other nodes as shown in Figure 3.

On the other hand the organization employees play different roles and each of them access the different resources with a specific security level as depicted in Figure-4. As a result the user access in the entire organization is the union of user-resource permissions for all user accessible resources. The administrators should always be aware of this spread of accesses and avoid overriding an access rule when adding or modifying a rule/access. There have been some attempt to undertake this complexity by introducing resource directories and uniform resource management protocols, but such approaches are not

[1] SOPA was proposed to JAX Innovation Award 2006 and nominated as one of top ten proposals for the final round together with famous frameworks like Spring and Rich Ajax Platform.

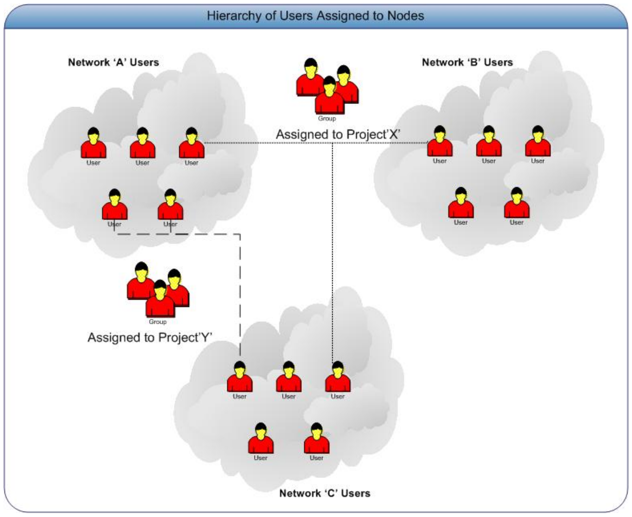

Fig. 4. User Assignment to Nodes

usually followed in heterogeneous system environments.

While working in networked environment it is quite possible that a node (individual computer or server) come under attack because of viruses, hackers, fire, vibrations, weak network policies or loopholes in software programs and operating system. For a node to be vulnerable, it has a precondition followed by an impact or aftereffects. There is a numbers of preconditions for a node to be exposed to vulnerability. Below are some use-cases for the type of attacks on a node in a networked environment followed by the reasons and aftereffects.

- Node 'a' comes under virus attack, preconditions for this kind of attack are missing of proper antivirus client, old virus definition or some patch is not updated.
- In networked environment open ports give passage to hackers to attack the network, resulting loss of information (confidentiality, integrity and availability). The precondition for this kind of attack can be data communication ports etc.
- Installation of malicious softwares on nodes can cause vulnerability. Intruders can get access easily. The precondition for such attack can be installation of P2P communication software for data transferring.
- In organizations where project is distributed on different nodes, concurrent versioning system plays an important role; the purpose of such system is to share the files in workplace. Sometimes because of weak rights, unauthorized person get access to confidential data.
- In an organization, website is hosted at different location. For example, database of the website at database server while information pages on some application server. If the database is not properly secured then attacker can penetrate causing damages

To name few there are some other means by which a node is exposed to vulnerability, like weak cryptography, inadequate password management and easy access to facility.

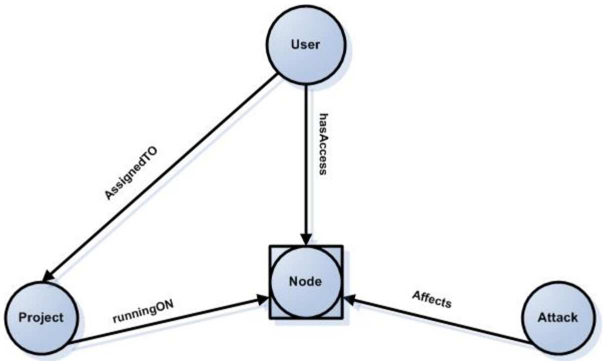

Fig. 5. Business entities relation

The impacts or aftereffects for vulnerabilities explained above are destroyed files, exposed data, lost productivity, lost machine control, wasted IT staff time to rebuild machine.

In project development environment of an organization the interaction between different business entities like user, project, node and attack is depicted in Figure 5.

Users are assigned to projects. Projects are running at different nodes. To have access to projects, users are assigned to nodes with roles depending upon their job description. Nodes are attached to each other through network. In distributed project environment nodes are grouped like, developer nodes, programmer nodes, manager nodes and server nodes etc. In network environment, nodes get exposed to attacks. Various reasons for this node to get exposed to attack and vulnerabilities are explained above. In organizations ultimate solution is risk assessment of attacks, which provides basis for the prevention from attacks in future. To put it in a nutshell the basic problem encountered in such environment is "to manage some very dynamic creatures that are highly sensitive, distributed and interconnected".

## VI. Use of ontologies

As explained earlier, our approach to calculate risk assessment is based on ontologies. To furnish this task we have divided the ontologies into three parts, i.e. (a) user environment ontology, (b) project ontology and (c) attack ontology. Figure 6 shows the high-level clases of these ontologies.

The user environment ontology captures the concepts of an environment in which users are working. By environment we mean the kind of operating system that is installed on the node, the kind of softwares that are in use and configuration of hardware at node, etc. A more detailed view of this ontology has been depicted in the Figure 7.

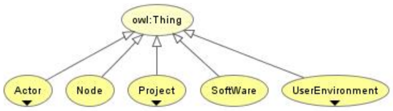

Fig. 6. High Level Ontology

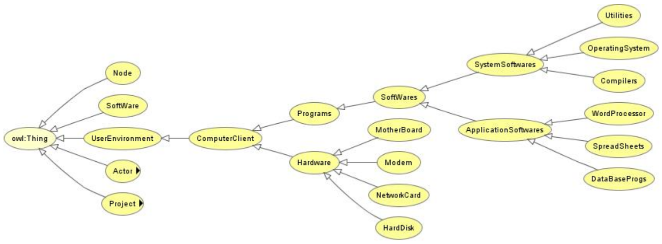

Fig. 7. User Environment Ontology

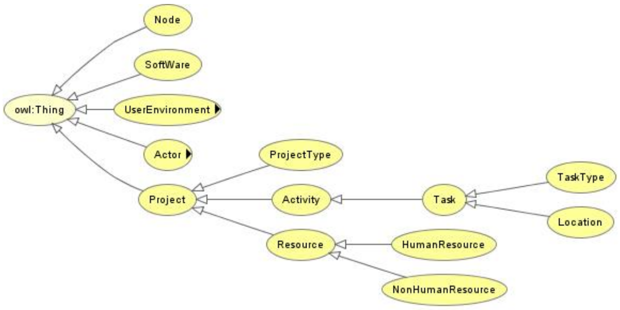

Fig. 8. Project Ontology

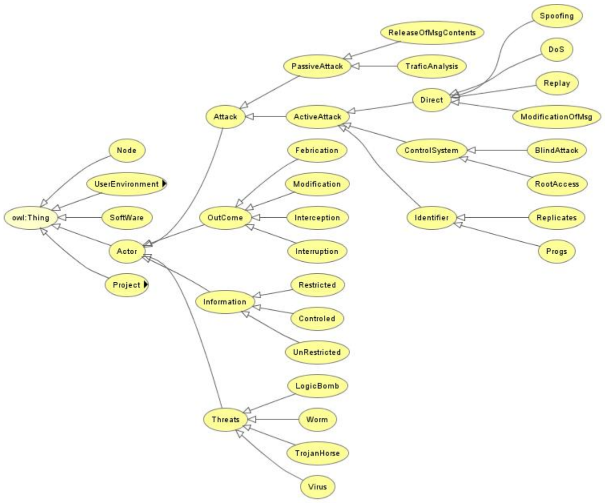

Fig. 9. Attack Ontology

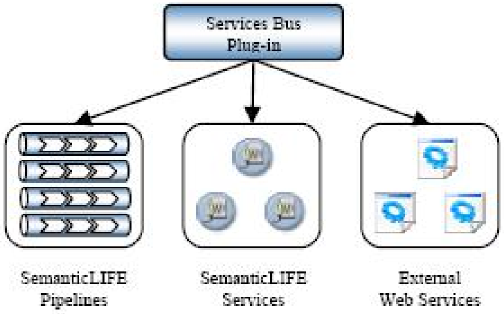

Fig. 10. Web Service plug-in services

Project ontology as shown in Figure 8 describes the taxonomy of project-related entities such as tasks, project plans, assignments & allocations, resources, and costs.

Attack ontology shown in Figure 9 is the main focus, which describes the different kind of attacks possible, like active and passive attacks, which are different preconditions for attack, which is the outcome of an attack etc. All these ontologies are mapped onto organizations' high level ontology, so that they can be used as the common mean of information sharing. On the other hand it provides a solid base that can be used by organization to translate the processes in a way that computers can interpret and apply them as business rules. As a matter of fact, business entities will be machine processable after being enriched with organization ontology.

## VII. Proposed Solution

In this section we will explore the proposed solution to collaborative risk assessment in an organization. First of all the core components of SemanticLIFE framework that play an important role in the proposed solution will be introduced.

SemanticLIFE is built on on several plug-ins components which communicate via the messaging and collaboration component. Message Bus, Web Service and Pipeline plug-ins are the fundamental plug-ins support of the communication framework.

- Message Bus plug-in manages all information exchanges between the SemanticLIFE processes. This plug-in also supplies a level of abstraction between systems services by providing a transparent, uniform access interface to all services.
- Web Service plug-in (Figure 10), uniforms all available resources as services and expose them to intern or extern user based on semantic policies and filters. Resources exposed by the Web-Service plug-in can be of the following types:
  - External web services that can be plugged to SemanticLIFE system at any time by locating the corresponding service description (WSDL files URL). More importantly, the plug-in supports capturing the semantic of a service which can be later on used during the contract making mechanism of business processes. The semantic of a service is defined in OWL-S standard and describes the functions of the service in terms of the transformation affected by the accordant service. It also specifies required inputs, pre-condition to invoke a service, the generated outputs, and the expected effects that result from the execution of the service.
  - Internal SemanticLIFE services that are primary built-in services of SemanticLIFE are used by other framework components. Examples of such services are semantic query, annotation and storage services. Internal services can be also extended by advanced users to customize the environment for their special

```
<pipeline name="spams">
<parameters>
<parametername="startDate" type="Date"/>
 <parametername="endDate"  type="Date"/>
</parameters>
<callid="mailSpams"service="at.slife.query"
     operation="mailQuery"/>
   <parameter>{startDate}</parameter>
  <parameter>{endDate}</parameter>
</call>
<callid="filtered"ervice="at.slife.filter"
     operation="dropNode"/>
<parameter>{xpath:/result/mailSpams}</parameter>
 <parameter><![CDATA[
     mailitem/@domain="bogous-domain"
      ]]> </parameter>
</call>
<transform xsl="summarize.xsl"/>
<serialize type="xml"/>
</pipeline>
```

Fig. 11. Simple Pipeline

```
< pipeline name="dengrousSpam">
< parameters>
<parametername="startDate" type="Date"/>
<parametername="endDate" type="Date"/>
<parametername="subnet" type="String"/>
</parameters>
<callid="workstations"service="at.slife.query"
      operation="workstationQuery"/>
< parameter>{subnet}</parameter>
</call>
<xsl:for-each select="/result/workstations/
    item">
<call id="mailSpams_{xpath:wsID}"
    service="at.slife.webservice@
{xpath:IPAddress}" operation="spams"/>
<parameter>{startDate}</parameter>
<parameter>{endDate}</parameter>
</call>
<transform xsl="spamReport.xsl"/>
<serialize type="html"/>
</pipeline>
```

Fig. 12. Administrator’s pipeline to access workstation services

needs.

  - SemanticLIFE pipelines is a mechanism to compose more complex services from primary services. The pipelines are also used for filtering the results based on user privacy and security policies.

- Pipeline plug-in that plays a central role in the proposed solution and aims to orchestrate basic system services and create new business services. We introduce the notion of a pipeline as an uniquely named set of service-calls and intermediate transformations. The pipelines are defined using an XML structure that specifies pipeline steps and relevant transformations. Listing in Figure 11 shows a simple pipeline that uses the internal SemanticLIFE services to get the Spam Emails from a workstation running SemanticLIFE.

The authorization process starts when Person-P1 requests Person-P2 to show a list of authorized documents. Person-P2 has full access to accept or deny a request, however persons can add or delete some documents related to the project for an authorized list depending on the confidentiality status. An important feature of pipelines is that they can be shared with other users based on user/administrator defined security policies. As an example the above defined pipeline can be installed in each workstation (inside the SemanticLIFE ecosystem) and report the spam from a specific domain to system administrator. At the administrators’ side there will be a similar situation and a pipeline will make a call to each workstation and will combine the results and will display the summary to administrator. The Listing in Figure 12 shows the administrator’s pipeline for this scenario.

As shown in the listing above, the pipeline concept offers many flexible features and complex scenarios can be described in terms of pipelines.

### A. Semantic Filtering

The SemanticLIFE services open the workstation services to the outside world. So there is a need for taking care of the users’ privacy and security issues. Figure 13 shows the security and privacy scenario in SemanticLIFE. The relevant information should be provided to authorized people only. One way of defining such authorizations is to use ontologies and find out the relationship between items and users. For example project ontology can tell us that a person is a project member, so he/she should be able to access all items (mails, files, photos, etc) on local computer that are tagged to be shared with project colleagues. The other usage of such ontological authorization rules is to filter the outgoing data. Some typical filters to services are.

- Content filter (filters all items containing a specified term, statement)
- Semantic filter (filters all project related documents)
- Annotation filter (filters all photos annotated by specific term like Class Diagram, ERD, etc)

Each filter performs a specific task; e.g. Semantic filter will filter the documents which are related to a project the relation of user who has requested the information with project. Annotation filter will filter the information item; e.g. filter the email with annotation project (X) or pictures with annotation ERD. For developing filters we need to specify which kind of information objects need to be filtered and then the inference engine will verify which information objects can pass through and be available to the requested person.

Ontology and inference engine are the basis for semantic filtering. The ontology is represented in formal language like OWL which captures the key concepts and relationships in the domain of interest, for example, in the project we have concepts like emails, documents and tools.

### B. Policy Implementation

In an organization, people have different types of access to the resources depending on their job description. In collaborative environment where people work together access to resources should be allowed based on defined policy and privileges. In collaborative environment where people works in groups, to accomplish their tasks it is essential that they have privileges over certain resources.

In SemanticLIFE information in the semantic store will be handled through policies.Policies are stored in the triple store in the form of RDF, which will facilitate how data should be handled i.e. who has access to which information and for whom data is restricted. Also information about how data was handled previously will be stored in the semantic store to facilitate user for decisions in future. Information in triple store will be handled through access control component and the user will be able to modify, delete or add policies through interface.

Numbers of policies can be implemented according to the collaborative environment. The user defines the policy for some specific operation, e.g. project resource sharing policies, project member access policies, stakeholder access policies etc. Take an example where the Person-P1 asks for documents related to the project. Person-P1 can be granted access if he/she is a member of that project and his/her status matches to the confidentiality of that document. There are number of candidate policy implementation languages like SWRL [17], KAoS [18] and REI [19]. We are still in the exploring phase for best suitable policy language which meets the requirements of our project. Figure below shows different components of SemanticLIFE and how policies and filters are used to control the information flow between SemanticLIFE-enabled workstations.

## VIII. Ontology-based risk assessments

In this section we will explore a risk assessment method based on SemanticLIFE toll for organizations' security which is a fundamental issue for planners and decision makers in IT field. As explained in the previous sections SemanticLIFE gathers the user interaction events and correlates those using ontologies. In the following sections, it will be explained how SemanticLIFE components can be employed to deliver the required input for risk assessment at organization level.

### A. Data capture and Event correlation

SemanticLIFE provides an effective approach to capture user interaction with computer. Such information can be analyzed and correlated with other events to establish a security profile for a single users' personal computer.

As an example, based on RDF repository, the following items can be identified:

- the applications that are installed on the system and their version
- the processes that are running on the system
- Browsed pages can be monitored and tracked
- Emails and spams

Combining this data with risk ontology, useful results can be generated. For example, from the risk ontology we know that a specific attack can happen only when specific preconditions are met. Some typical preconditions are, OS version, open ports, etc.

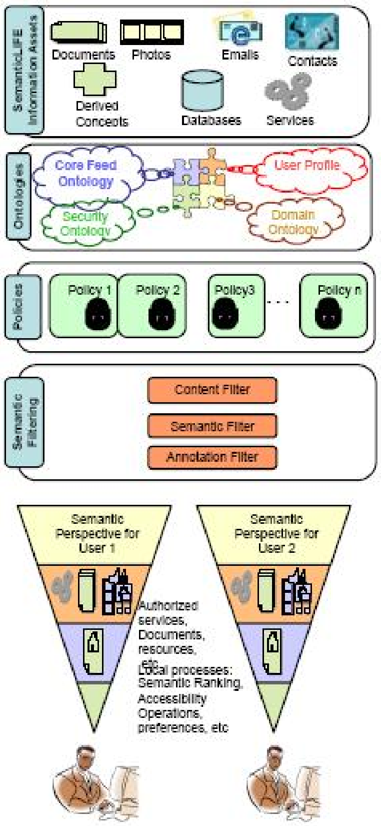

Fig. 13. Security and Privacy scenario in SemanticLIFE

### B. Collaboration at organizational-level

Maintaining and monitoring the computer networks and nodes is a big challenge for system administrator and organizations. Keeping an eye on all computers and detecting the attack vulnerable in big organizations is nearly impossible.

SemanticLIFE architecture provides a mechanism to expose the risk factors to the system administrator who is responsible for securing the system. This can be realized via some pipelines on clients that assess required information and share them in a "Service Oriented"-like paradigm. Such a scenario was demonstrated in previous sections.

As proof of concept we show how the SemanticLIFE paradigm can be used to assess a typical quantitative risk assessment method that is used to assess the risk factor in organization. Quantitative methods generally use the available data to give a numerical description of the risk. One such quantitative method is shown in Figure-14 for calculating the Annual Loss Expectancy (ALE) that has been introduced in Common Framework. According to definition the Annual Loss Expectancy is the estimation of the yearly potential loss of an organization if the risks are not handled. The ALE is calculated as follows:

$$ALE = \sum_{i=0}^{n} I(O_i)F_i \qquad (1)$$

where $O = \langle O_1, O_2, \ldots O_n \rangle$ is a set of *harmful outcomes*, $I(O_i)$ is the *impact* of outcome $O_i$ in US dollars, and $F_i$ is the frequency of $i$th outcome. In the equation 1 the set of harmful outcomes and also the impact of each outcome can be estimated, however the frequency of the outcome can not be easily known and this makes the ALE coarse and not easy to calculate. However using the SemanticLIFE paradigm we can feed the ALE calculation process by the input from real events and as a result the ALE will be more realistic.

The same method can also be applied to the project to calculate the project risk. In this case we might user the project and environment ontology to do the task. The following steps are needed to fulfill the task:

- The network nodes that might affect the specified project will be extracted from ontology
- From the risk ontology we will know which risks are conceivable for each node and we can assess the set of harmful outcomes.
- By setting up the appropriate pipelines the organization-wide data can be gathered and fed into risk assessment algorithms (ALE for example)

Using the similar method we can assess the risk for computer/user groups and answer questions like:

- Which department has the highest risk?
- Which project is at the highest risk?

### C. Privacy issues

Though the presented method seem to be very powerful to control and maintain the organization network and nodes, but it is important to take the privacy issues into consideration. Probably a part of the information that is going to be shared should be depersonalized first. This process can be also supported by the ontology of the items that is going to be shared and by the sensitivity of information. As explained before some privacy issues can be addressed by policies and semantic filters.

## IX. Conclusion and future work

Semantic Web technology has opened a new window in IT and especially in data engineering fields. The proposed scenario suggests that technology can be used to make the daily life scenarios easier to organize. The presented SemanticLIFE platform has the capacity to be used in other business processes dealing with personal information (local data, resources, etc). The SemanticLIFE platform also proposes a paradigm to manage the security and privacy issues of information and process sharing. After a secure and robust share of such information, it is possible to assess organizational-level factors such as risk factors.

Some other challenging module like Semantic Web Services is still under development progress and we try to enhance the features and keep up with the latest advances. The SemanticLIFE domain ontology is also evolving and aimed to be empowered by the known risk, user profile and infrastructure ontologies.

## Acknowledgment

The work presented in this paper is partially supported by ASEA-UNINET (ASEAN-EU Academic University Network) and also by HEC (Higher Education Commission of Pakistan). The authors would like to acknowledge the support of the SemanticLIFE team. The work presented here is result of various group discussions and implementation by the team members.

## References

[1] "Information security risk assessment – practices of leading organizations," United States General Accounting Office (GAO), Executive Guide GAO/AIMD-00-33, November 1999, http://www.gao.gov/special.pubs/ai00033.pdf.

[2] S.-W. Lee, R. Gandhi, D. Muthurajan, D. Yavagal, and G.-J. Ahn, "Building problem domain ontology from security requirements in regulatory documents," in *Proceedings of International Workshop on Software Engineering for Secure Systems*. ACM Press, 2006, pp. 43–50.

[3] B. Tsoumas, S. Dritsas, and D. Gritzalis, "An ontology-based approach to information systems security management," in *Proceedings of International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS)*, ser. Lecture Notes in Computer Science, vol. 3685. St. Petersburg, Russia: Springer Verlag, September 2005, pp. 151–164.

[4] S. Liu and L.-F. Kwok, "Data integration framework for a knowledge model of organizational information security management," in *Proceedings of 2nd Secure Knowledge Management Workshop (SKM)*, September 2006.

[5] B. Tsoumas and D. Gritzalisi, "Towards an ontology-based security management," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA)*, Vienna, Austria, April 2006, pp. 985–992.

[6] M. Klemen, E. Weippl, A. Ekelhart, and S. Fenz, "Security ontology: Simulating threats to corporate assets," in *Proceedings of the 2nd International Conference on Information Systems Security (ICISS)*. Springer, 2006, pp. 249–259.

[7] A. Simmonds, P. Sandilands, and L. van Ekert, "An ontology for network security attacks," in *Proceedings of Asian Applied Computing Conference (AACC)*, ser. Lecture Notes in Computer Science, vol. 3285. Kathmandu, Nepal: Springer Berlin, October 2004, pp. 317–323.

[8] P. Mitra, C. Pan, P. Liu, and V. Atluri, "Privacy-preserving semantic interoperation and access control of heterogeneous databases," in *Proceedings of Symposium on Information, computer and communications security*. ACM Press, 2006, pp. 66–77.

[9] H. Li, X. Zhang, H. Wu, and Y. Qu, "Design and application of rule based access control policies," in *Proceedings of Semantic Web and Policy Workshop*, Galway, Ireland, November 2005, pp. 34–41.

[10] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments," in *Proceedings of 5th International Semantic Web Conference*, ser. Lecture Notes in Computer Science, vol. 4273. Athens, GA: ACM Press, November 2006, pp. 473–786.

[11] A. Toninelli, J. M. Bradshaw, L. Kagal, and R. Montanari, "Rule-based and ontology-based policies: Toward a hybrid approach to control agents in pervasive environments," in *Proceedings of the Semantic Web and Policy Workshop*, Galway, Ireland, November 2005, pp. 42–54.

[12] T. Berners-Lee, J. Handler, and O. Lasilla, "The semantic web," *Scientific American*, May 2001, http://www.sciam.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21.

[13] B. Thuraisingham, "Security issues for the semantic web," in *Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC03)*. IEEE Computer Society, November 2003, pp. 633–638.

[14] ——, *Xml Databases and the Semantic Web*. CRC Press, FL, 2001.

[15] A. Kim, L. J. Hoffman, and C. D. Martin, "Building privacy into the semantic web: An ontology needed now," in *Proceedings of International Workshop on the Semantic Web*, Hawaii, USA, May 2002, semanticweb2002.aifb.uni-karlsruhe.de/proceedings/Position/kim2.pdf.

[16] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, "The p3p specification," W3C, Recommendation 1.0, 2001, http://www.w3.org/TR/2001/WD-P3P-20010928/.

[17] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, and M. Dean, "Swrl: A semantic web rule language combining owl and ruleml," 2004, http://www.w3.org/Submission/SWRL/.

[18] A. Uszok, J. M. Bradshaw, M. Johnson, and R. Jeffers, "Kaos policy management for semantic web services," in *Proceeding of IEEE 4th International Workshop on Policy*. IEEE Computer Society, July/August 2004, pp. 32–41.

[19] T. F. Lalana Kagal and A. Joshi, "A policy language for pervasive computing environment," in *In Proceeding of IEEE fourth International Workshop on Policy*. Italy: IEEE Computer Society, June 2003, pp. 63–76.