

SCENS: a System for the Mediated Sharing of Sensitive Data

Song Ye, Fillia Makedon, Tilmann Steinberg, Li Shen,
James Ford, Yuhang Wang and Yan Zhao
DEVLAB, Computer Science Department, Dartmouth College
{yesong, makedon, tilmann, li, jford, wyh, yanzhao}
@ cs.dartmouth.edu

Sarantos Kapidakis
Department of Archive and
Library Sciences,
Ionian University, Greece
sarantos@ionio.gr

Abstract

This paper introduces SCENS, a Secure Content Exchange Negotiation System suitable for the exchange of private digital data that reside in distributed digital repositories. SCENS is an open negotiation system with flexibility, security and scalability. SCENS is currently being designed to support data sharing in scientific research, by providing incentives and goals specific to a research community. However, it can easily be extended to apply to other communities, such as government, commercial and other types of exchanges. It is a trusted third party software infrastructure enabling independent entities to interact and conduct multiple forms of negotiation.

1. Introduction

The aim of SCENS (Secure Content Exchange Negotiation System) is to facilitate data sharing through negotiation on metadata information derived from data of interest (“primary data”). Primary data exchange is done between two parties once they have reached agreement, and, until then, primary data remain in the control of data owners. Applications of this model include banks, scientific repositories and film archives. For convenience, we will use the term *digital libraries* to encompass these and other potential applications.

SCENS was originally designed and implemented to support data sharing in neuroscience research, where sharing is important in promoting discovery and collaboration. Neuroscience data are not only private but also of high value due to production costs. Traditionally, researchers have resisted sharing primary data in this field. Our efforts are synergistic with ongoing efforts (e.g. BIRN [1]) because we provide a flexible, user-centered alternative to large, trans-national archiving of published-only results that provide limited access control to the data

owner once he has given the data. SCENS negotiation services provide a secure mechanism of reaching agreements on conditions for primary data sharing. In this respect, our system offers a novel way for digital libraries composed of sensitive data to grow while enhancing collaboration of users and providing data usage tracking facilities.

2. Related work

Several Web-based negotiation support systems are currently in use. SmartSettle [2] uses a central server to arrive at agreements without exposing confidential data. WebNS [3] is a prototype Web-based Negotiation System, designed to facilitate remote negotiations on the Internet. INSPIRE [4] is a Web-based negotiation support system containing facilities for specification and assessment of preferences.

However, most existing negotiation support systems do not have enough flexibility to support negotiation agents and automated negotiation. They also do not focus on security and scalability issues.

3. The Characteristics of SCENS

3.1. Flexible

SCENS has a flexible 3-layer service structure that provides different levels of negotiation services for different type of users.

Layer 1 behaves as a traditional web-based negotiation support system for human beings. It also provides some negotiation agents, which are actually user customizable utility functions. Users can customize the negotiation agents provided by Layer 1 through multiple parameters, such as the weights assigned to different negotiation conditions. However, the agents provided by Layer 1 are not fully customizable; if the negotiation strategy is very complex, it simply cannot be expressed by these parameters.

Layer 2 supports complete negotiation strategy customization by users. In Layer 2, users are allowed to have their own negotiation agents to implement any negotiation strategies. The negotiation agents, which are treated as web service consumers and run on the client side, conduct negotiation with other negotiation agents or human beings through web services. Figure 1 shows the interactivity between Layer 1 and Layer 2.

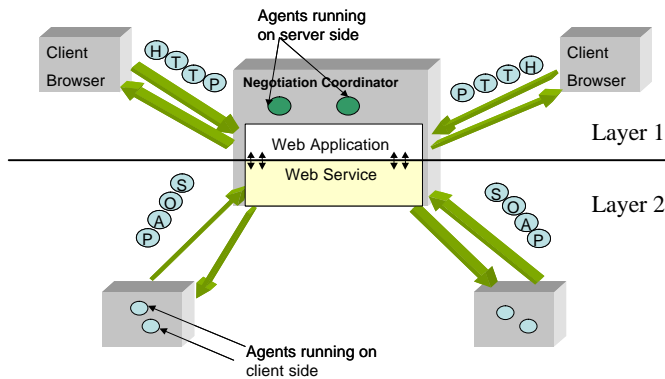


Figure 1. Layer 1 provides web-based negotiation services for human beings; Layer 2 interacts with negotiation agents through web services

Layer 3 is designed to provide an open and automated negotiation environment. DAML+OIL [5][6], a language for creating ontologies and marking up information, is used in Layer 3 to define a negotiation ontology, which allows agents to acquire knowledge about how to conduct negotiations. This knowledge includes negotiation protocols, negotiation proposals and conditions, etc. Agents communicating with Layer 3 can be used in any negotiation activities given the proper negotiation ontology. In Layer 2, in contrast, the knowledge about negotiation rules is actually hard-coded into the agents.

3.2. Secure

Security issues in SCENS involve a trade-off between access and access control. In addition to the traditional triad of confidentiality, integrity, and availability, SCENS introduces the desire to control data rights when one gives the data to another and the need to analyze and compose policies under which data may be shared.

Even though SCENS handles metadata only, privacy issues still must be addressed—for example, aggregation attacks. SCENS can provide tracking of data usage, analysis of the statistical security of data, and traffic analysis to prevent this kind of attacks.

Availability is more difficult to handle. A denial of service attack could easily disrupt negotiations, especially in SCENS, where users are allowed to provide their own negotiation agents running on clients. The negotiation protocol has been constructed to minimize the ability of denial of service attacks to disrupt the negotiations. However, SCENS is still vulnerable under denial of service attacks against the protocols underlying the negotiation protocol (such as TCP and IP).

3.3. Scalable

The deployment of SCENS supports a hierarchical structure. When inter-domain (the notion of domain is very flexible, and can be departments, labs or groups) negotiation is desired, a negotiation party in one domain cannot directly negotiate with a party in another domain; it can only communicate through the SCENS server in its own domain. A SCENS server in a domain only trusts other servers or users in its own domain. Figure 2 shows an example.

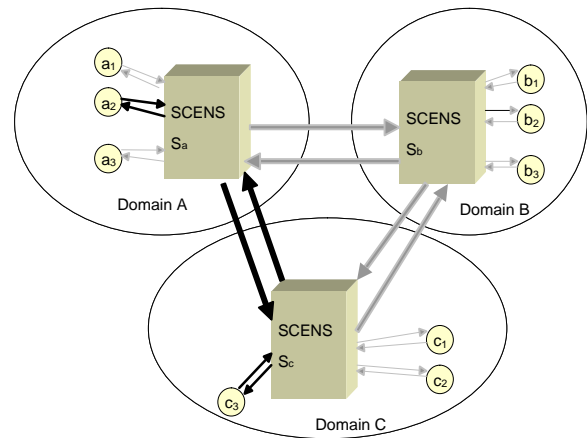


Figure 2. a₂ and c₃ are negotiating

4. How SCENS Works

In [8], an application of SCENS, the Data Broker Framework (DBF), is introduced to automate object acquisition, as well as support decision-making in obtaining the best “data collection deal”. DBF tracks collection needs, past transactions, “bargain” for the best conditions, and promotes a common standard for computer-mediated negotiation involving diverse parties.

Based on SCENS, DBF helps any type of collector such as scientific databases, digital libraries, business records, and film archives, to collect content they need.

Figure 3 shows the use of SCENS. As noted earlier, SCENS is responsible for supporting and authenticating negotiations on data exchanges. After agreement is reached, any data exchange is beyond the control of SCENS. However, feedback on the data shared is reported back to SCENS, thus enabling the system to perform user and data tracking.

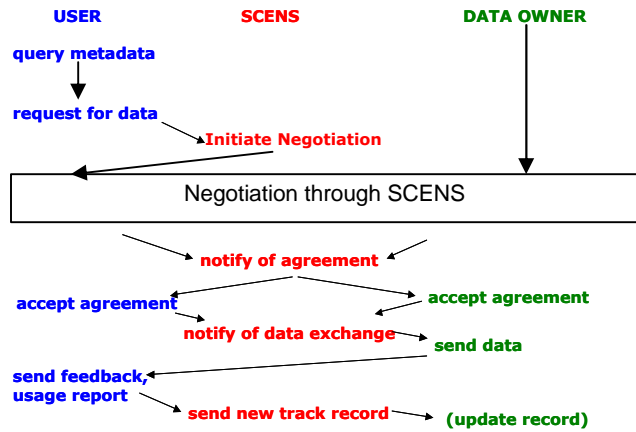


Figure 3. How SCENS works

5. System Implementation

In our implementation of SCENS, we used AXIS (version 1.0rc2), a SOAP implementation from Apache Software Foundation, to provide negotiation web services (Layer 2). Our web-based negotiation service (Layer 1) is implemented using JSP 1.2. For Layer 3, we are building ontologies for brain tumor research using DAML+OIL and developing agents which interact with Layer 3.

The system is still under development. The services implemented include *user authentication*, *data quality assessment*, *web-based negotiation* (Layer 1), *web service based negotiation* (Layer 2), *usage tracking*, *user evaluation* and other services. We have also developed synthetic tools to simulate the negotiation activities and help evaluate the whole system. Figure 4 shows a partial list of implemented web services; Figure 5 shows a portion of the web-based interface supporting multi-user negotiations.



Figure 4. SCENS web services for Layer 2

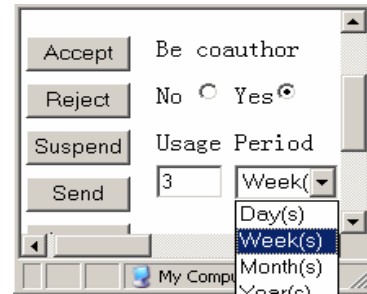


Figure 5. The SCENS interface for Layer 1

6. Conclusion and future work

Our work builds on earlier work on MetaDLs [7, 9]. SCENS not only can be used to support negotiation activities, but also serves as a testbed for testing different negotiation strategies (Layer 2) and automated negotiation (Layer 3). Our next work is primarily in Layer 3. We are currently building applicable negotiation ontologies for information sharing and will extend these to a general-purpose approach. The long term goal of SCENS is to support fully automated negotiation for sensitive data sharing.

References

- [1] <http://www.nbirn.net/> Visited 3/30/2003
- [2] <http://www.oneaccordinc.com/> Visited 3/30/2003
- [3] <http://webns.mcmaster.ca/> Visited 3/30/2003
- [4] Kersten G., Noronha S., Supporting International Negotiation with a WWW-based System. Internet Research Report INR05/97, 1997
- [5] Hendler J., McGuinness D.L., The DARPA Agent Markup Language, IEEE Intelligent Systems, vol. 16, no. 6, Jan./Feb., 2000, pp. 67-73
- [6] <http://www.daml.org/2001/03/daml+oil-index> Visited 3/30/2003
- [7] Makedon F., Ford J., et al., MetaDL: A Digital Library of Metadata for Sensitive or Complex Research Data, ECDL'02, Sept. 2002, Rome, Italy.
- [8] Makedon, F., Kapidakis, S., et al., Data Brokers: Building Collections Through Automated Negotiation, Dartmouth College Computer Science Department, Hanover, NH, Technical Report DEVLAB-SCENS-03-02, March 2003.
- [9] Ford, J., Makedon, F., et al., Evaluation Metrics for User-centered Ranking of Content in MetaDL, Fourth DELOS Workshop on Evaluation of Digital Libraries: Testbeds, Measurements, and Metrics, Budapest, Hungary, May 6-7, 2002