implementation, which allows for existing infrastructure (e. g. an XMPP server used for instant messaging) to be reused. Additionally, the Google Wave project [18] demonstrated the use of the Operational Transformation (OT, [19]) scheme for real-time collaborative editing across XMPP federations.

XMPP clients can also be used to interface with resources in order to enforce access control configurations or delegate policy decisions to the server. For example, using SPARQL queries (see below), we can easily extract a list of users that have been granted access to a MySQL table by the policies in the Mind Mesh and send it to the Mind Mesh client (cf. Fig. 3) on the corresponding machine. The client then issues SQL queries granting access to tables accordingly.

The Mind Mesh graph itself is stored as Resource Description Framework (RDF) triples, since graph relationships between nodes directly correspond to the *subject – predicate – object* paradigm of RDF. Furthermore, the graph's structure can be comfortably interrogated using SPARQL queries. Additional semantics can be incorporated using a reasoner and an ontology language, such as OWL. The ontology contains concepts and properties relevant to model access control, such as *Policy* or *hasReadAccess*, but also incorporates domain specific knowledge that can be maintained by the users. The Mind Mesh prototype UI is browser based, since this significantly reduces the deployment and management effort and facilitates adoption of the Mind Mesh approach, especially with non-ICT-native users.

VII. Conclusion

In this paper, we presented a requirement analysis and novel concept for an intuitive visual access control solution in research ecosystems. The requirements of cross-organisational and cross-domain AC management solutions for digital research ecosystems were identified and discussed. Based on this discussion a design of a prototype concept was outlined. The design couples expressive access control models with visual information of the underlying ecosystem resources. We proposed a collaborative graph-based system called Mind Mesh, allowing every actor in the ecosystem to contribute to the management of the environmental information. By operationalising this information, users are enabled to intuitively configure AC policies across a heterogeneous ecosystem infrastructure. In particular, the Mind Mesh approach integrates legacy software systems in a bottom-up fashion and therefore greatly reduces configuration overhead for short-lived and ad-hoc collaborations. To protect the AC policies, a design for an integrated meta-policy concept was presented. Using the ecosystem information captured in the Mind Mesh graph, AC rules can be visualised and explained, hence significantly easing the management of complex research ecosystems.

There are several areas of future work to extend the presented simple prototype. Currently, the concepts available for capturing context are part of a predefined ontology. In the future, the users should be allowed to adapt the underlying ontology to the needs of their domain. Allowing users to specify custom concepts for the AC system will significantly broaden the scope and increase the flexibility. The intuitiveness of visualising access control information in research ecosystems will diminish the larger and more complex the ecosystems become. Therefore, smart views will be needed, which allow a combination of user selected views and algorithmically selected information subsets that focus the user on the matter at hand without hiding relevant details. Finally, a framework for protecting the Mind Mesh plugins based on the context in the Mind Mesh needs to be designend and implemented as well.

References

[1] D. Regan, O. Pusatli, E. Lutton, and D. Athauda, "Securing an EHR in a Health Sector Digital Ecosystem," in *3rd IEEE International Conference on Digital Ecosystems and Technologies*, June 2009, pp. 285–289.

[2] T. Buzan, *Make the Most of your Mind*. Pan Books, 1977.

[3] E. Nankani, S. Simoff, S. Denize, and L. Young, "Enterprise University as a Digital Ecosystem: Visual Analysis of Academic Collaboration," in *Digital Ecosystems and Technologies*, June 2009, pp. 727–732.

[4] The SWAP Project, http://swap.semanticweb.org/, 2004, last accessed on 07.01.11.

[5] S.-A. Katriou, E. Tolias, and A. Mavridis, "A European Union Research Partner Collaboration Creation System," in *3rd IEEE International Conference on Digital Ecosystems and Technologies*, June 2009, pp. 547–551.

[6] G. Fragidis, A. Mavridis, A. Vontas, A. Koumpis, and K. Tarabanis, "A Proposed Conceptual Framework for the Study of Research Ecosystems," in *2nd IEEE International Conference on Digital Ecosystems and Technologies*, February 2008, pp. 71–76.

[7] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *Computer*, vol. 29, pp. 38–47, February 1996.

[8] J. L. D. Coi and D. Olmedilla, "A Review of Trust Management, Security and Privacy Policy Languages," in *International Conference on Security and Cryptography*, Jul. 2008.

[9] E. Yuan and J. Tong, "Attributed based access control (ABAC) for Web services," in *IEEE International Conference on Web Services*, July 2005, p. 569.

[10] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting Attribute-based Access Control With Ontologies," in *The First International Conference on Availability, Reliability and Security*, April 2006.

[11] T. Ryutov, T. Kichkaylo, and R. Neches, "Access Control Policies for Semantic Networks," in *IEEE International Symposium on Policies for Distributed Systems and Networks*, July 2009, pp. 150–157.

[12] N. Elahi, M. Chowdhury, and J. i. i. i. Noll, "Semantic access control in web based communities," in *The Third International Multi-Conference on Computing in the Global Information Technology*, August 2008, pp. 131–136.

[13] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A Semantic Web Based Framework for Social Network Access Control," in *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, 2009, pp. 177–186.

[14] L. Kagal, T. Berners-Lee, D. Connolly, and D. Weitzner, "Self-describing Delegation Networks for the Web," in *Seventh IEEE International Workshop on Policies for Distributed Systems and Networks*, June 2006.

[15] V. Geroimenko and C. Chen, Eds., *Visualizing the Semantic Web – XML-Based Internet and Information Visualization*, 2nd ed. Springer London, 2006.

[16] The XMPP Standards Foundation, http://xmpp.org/.

[17] P. Saint-Andre, *XEP-0114: Jabber Component Protocol*, http://xmpp.org/extensions/xep-0114.html, XMPP Standards Foundation Std., Rev. 1.5, 2005.

[18] D. Wang, A. Mah, and S. Lassen, "Google Wave Operational Transformation," Google Inc., Tech. Rep., July 2010. [Online]. Available: http://wave-protocol.googlecode.com/hg/whitepapers/operational-transform/operational-transform.html

[19] C. Sun, Y. Zhang, X. Jia, and Y. Yang, "A Generic Operation Transformation Scheme for Consistency Maintenance in Real-Time Cooperative Editing Systems," in *Proceedings of ACM SIGGROUP*, 1997, pp. 425–434.

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE