This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Ontology-based Risk Evaluation in User-centric Identity Management

Gail-Joon Ahn and Pradeep Sekar
Arizona State University
{gahn, psekar}@asu.edu

***Abstract*—Recent trends in the area of identity management have evolved from a traditional identification solution to a distributed user-centric identity management mechanism. The major goal of user-centric identity management is to enable the users to have control over their own digital identities. Even though existing identity management systems attempt to offer user-centricity where users possess complete control on their identity disclosure, however, it does not signify the consequences of the users' behavior. It is necessary to assist the users on the risk involved in disclosing their identity attributes. In this paper, we propose a risk-aware mechanism to help the users decide the degree of identity disclosure risk using ontology-based evaluation and privacy preference evaluation. We demonstrate the feasibility of our approach on dynamic online social networks where the user's identity plays a major role for access control and privacy management.**

I. Introduction

A wide range of web-based services have been created to provide various services to the users. Most of them require the users to prove their identity for ensuring information assurance and reliability. Trustability of the Service Provider (SP) depends on how legitimately they manage the users' identity information and corresponding privacy preferences. Traditionally the SPs collect and manage the users' identity information which are prone to identity theft and other privacy violations. In addition, the current architecture cannot fully accommodate the important role played by the users in the process of identity disclosure. In a distributed model, the users possess complete control in managing and disclosing their identities via trusted third-party Identity Providers (IdPs). For instance, Liberty Alliance [4], OpenID [16], CardSpace [5] and Higgins [1] also focus on user-centric identity management requiring a user to obtain prior knowledge and responsibility in deciding the credibility of SPs and their data practices to handle identities.

Online Social Networks (OSNs) provide dynamic information sharing and trustable human network. Users disclose a subset of their personal profile as identity information to get various services from the SPs. The identity information depends on the context of the service the user requests, such as the employee number for an employer community, student ID for a University, and so on. Also, applying traditional identity models such as password-driven [8] or secret credentials may not be sufficient enough to determine trustworthiness of SPs.

Despite providing ownership on their identities, user-centricity holds the users responsible for handling and managing their information across Internet. As a user agent (UA) negotiates with the SP and IdP during the identity disclosure, they can be extended with intelligent agents which can suggest the user about the risk involved in disclosing certain identity information to the SP. In this paper, we propose a mechanism to suggest the user with quantifiable risk values and provides a way to securely manage user identities involving trusted third-party IdPs and disclose them based on users' preferences. We first model an ontology of identity information to have a common understanding of identity attributes across various social networks. We adopt a web ontology language OWL [14] to construct an object-oriented relationship of identity attributes between various social networks. The prime objective of our ontology called identity attribute ontology (IAO) is to construct a class relationship of user identity information with which any generic notion can be applied and used by various components. Each *class* in the IAO represents an identity attribute. The *individual* represents an instance of the class which is the attribute representing their class in various online social networks. We also present a notion of risk such as personality and financial risks for every *class* or *individual* in the IAO. Every *class* or *individual* represents a numeric value for the associated risk which can be referred by various UA for evaluation risks involved with identity information disclosure. The IAO provides the similarity matching functionality where the identity information is analyzed to semantically find the best matching classes for their risk values.

User-centricity should also consider the users' preference in handling their identity information at the SP. Policy-based privacy has received significant attention in the distributed identity models which make the privacy expression more portable and platform independent. [2] proposed an approach where users' privacy preferences are collected based on the category of the identity attributes and the preferences are evaluated with the SP's privacy policies. Although the category-based approach has been successful in e-Commerce and other web applications, a user in an OSN platform tends to have different privacy preferences for the same identity attribute based on the domain. Hence, we need to group OSNs based on domains such as social, financial, federal government, etc while allowing the users to set privacy levels for each identity attribute accordingly. Privacy evaluation is performed based on both SP's privacy policies and a user's privacy preference for the domain which the SP belongs to.

The rest of this paper is organized as follows. Section II

978-1-61284-233-2/11/$26.00 ©2011 IEEE

describes the related work. The design and methodology of our approach are explained in Section III. Section IV presents implementation details of our proposed mechanisms with the results on social networks. Section V concludes the paper.

II. Related Work

Several researches have proposed standards for a trustable and usable Distributed Identity Model (DIM) for the evolving web architecture and modern collaborative applications. DIM redefines the practice of identity management by clearly specifying the roles and responsibilities of involving parties. User-centricity is one of the primary requirements of DIM which attempts to improve the user interaction and awareness during the transaction. Although it offers control over the identity disclosure, it is required for a user to possess enough knowledge to make decisions. In the Internet, a user's transactions often involve a questionable SP and the user does not have a systematic, quantifiable mechanism to ascertain their decisions on identity disclosures to the SP.

To help SPs publish privacy-related practices, several research work proposed ways to express privacy policies such as XML-based privacy expressive language, P3P (Platform for Privacy Preferences Project). AT&T Privacy Bird is one of the major initiatives in developing a user agent for P3P which works as a browser helper in a commonly used browser Internet Explorer [6]. They also proposed the standard for the user-agents which can provide privacy validation [7]. Several other researchers also proposed several features for DIM such as policy-based privacy validation in [2], [3]. Using semantic web technologies for user identity and privacy management was discussed in [9]–[11]. Developing Ontologies for user privacy attributes was also proposed in [9]. In this paper, we attempt to leverage policy-based privacy evaluation and the concept of semantic ontology focusing on identity attributes on OSNs.

III. Our Approach

This section describes how the risk evaluation can improve user privacy and provide better control on the identity disclosures to the SPs. We first summarize a procedure in releasing user identity to an SP as follows:

i) IdP manages and holds a user's identity related information.
ii) Upon the user's service request to a SP, the SP sends the user a list of attributes, called *requested attributes* (*RA*) necessary to provide the requested service.
ii) The user's UA checks the similarity between *RA* and classes in IAO to compute a list of releasable attributes, called *releasing classes RC*. In the matching process, UA also evaluates potential risks in releasing attributes of *RC*, and queries IAO to find *RC* which has the maximum semantic similarity with *RA*, while *RC* satisfies the minimum risk imposed by the user on an IAO.
iv) *RC* is presented to the user with the representation of associated risks. The user modifies and supplements *RC* if necessary. Some requested attributes x may not be included in the *RC*, because either the risk of x is intolerable to the user or the user declines the release of x. After SP and the user agree on *RC*, the information of *RC* is sent from IdP to SP.

IdP manages a number of identity attributes for the user, such as student ID, email addresses, credit card number and various attributes representing the user in social network services. Some of these attributes might be anonymous, while others directly present the user's persona. In selecting *RC*, UA needs to evaluate the combination of attributes with the lowest risk and the best similarity while avoiding any attribute linkages that should be prohibited based on the user preference. IAO can also provide the combined risk representation of attributes which helps in preserving anonymity if necessary.

A. Notion of Risk

Now we discuss the basic notions of the risk evaluation method with IAO.

Risk Value is a numerical scale of 1.0 to 5.0 representing the degree of severity, where 1.0 is the least severe and 5.0 is the most severe. Risk values are categorized into financial and personality risk values. IAO holds risk values in each class. However, some classes may not have the defined risk values. If a risk value of a class y is undefined, then the risk value is inherited from y's senior classes. If a class z is in the releasing class *RC*, then the risk values of z becomes *effective*. The risk value of releasing classes *RC* is the maximum effective risk value in the classes of *RC*.

Financial risk value (f-risk value in short) is a risk value for indicating financial damage to the information subject (user). Credit card number, bank account number, and social security number should have higher financial risk values. We use a function $r_f(.)$ to denote financial risk values on various constructs such as a class C and releasing classes *RC*.

Personality risk value (p-risk value in short) is a risk value for personality damage to the user, including emotional pain, damage to social reputation, and generic damage caused by privacy breach. We use $r_p(.)$ to denote the personality risk value function.

Combined risk value $r_c(RC)$ combines f-risk and p-risk values by the function $r_c(RC) = cr(r_f(RC), r_p(RC))$ such that $cr(\alpha, \beta) = c_1 log(F^\alpha + P^\beta) + c_2$, where the risk values α and β are converted into an exponential scale by the exponential functions of bases F and P, and the average of these values are converted back to risk values by the logarithmic function. Constants c_1 and c_2 shall be determined to let $cr(\alpha, \beta)$ have a range between 1.0 and 5.0.

Combination risk is a risk which arises from the combined release of the attributes in the transaction. Some identity attributes, such as SSN and employee id, may be disclosed under an anonymous username, whereas the combination of these attributes with the real username raises potential privacy breaches. Thus, the user should be notified of such a high risk involved in releasing the attributes. Also, the user holding a number of identity attributes at IdP can choose one attribute or a combination of attributes to present the requested attributes.

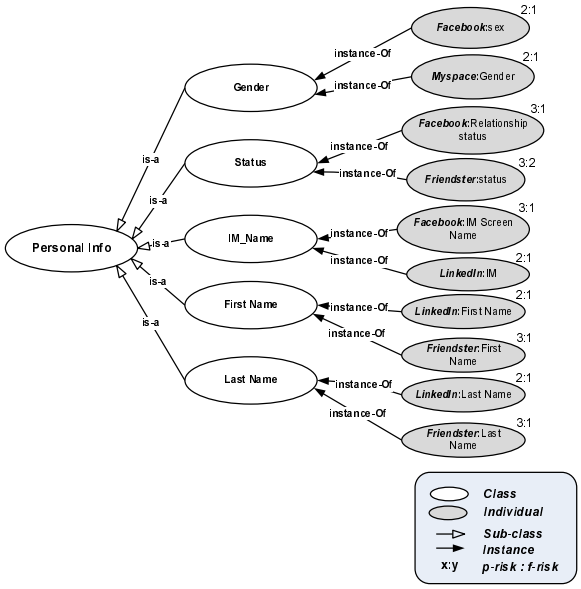


Fig. 1. Ontology of User Identity Attributes

In this scenario, the user should be advised of the risk in linking several identities.

Risk Limit is a given upper limit of f-risk, p-risk or combined risk values. If the user gives his/her tolerable risk limit, then disclosing attributes should not exceed the limit.

B. Modeling Identity Attribute Ontology

To formalize the identity attribute ontology shown in Figure 1, we adopt the definitions of OWL as the underlying model. Generic classes are identified in order to relate vocabulary representing user attributes from various service providers. A *class* represents a concept. An individual represents a user attribute from a service provider belonging to the associated class. A class is associated with zero or more *individuals* which are the instances of that class. An ontology can be represented as a directed graph, where nodes are labeled with a class name or an individual, and directed edges are labeled as link types. A link labeled *instanceOf* from an individual to a class represents the membership relation between the individual and the class. A link labeled *is-a* from class C_1 to class C_2 indicates that C_1 is a subclass of C_2 meaning that C_1 is a concept more specific that C_2 and an individual belonging to C_2 also belongs to C_1. A link labeled *partOf* from class C_1 to class C_2 indicates that C_2 is a *composite* class composed of a number of *component classes*, including C_1. Formally, if a class C_1 is connected to a class C_2 through a directed path of *partOf* and *is-a* links, then C_1 is a component class of C_2. *partOf* links are not allowed to form a directed cycle. We define *composite attributes* for requested attributes, similarly to composite classes.

IAO has two special link types named *financialRisk* and *personalityRisk*, representing the financial risk value $r_f(C)$ and personality risk value $r_p(C)$ of a class C, leading to individuals of real numbers in the range [1.0, 5.0]. An example of identity attribute ontology is shown in Figure 1, where risk values

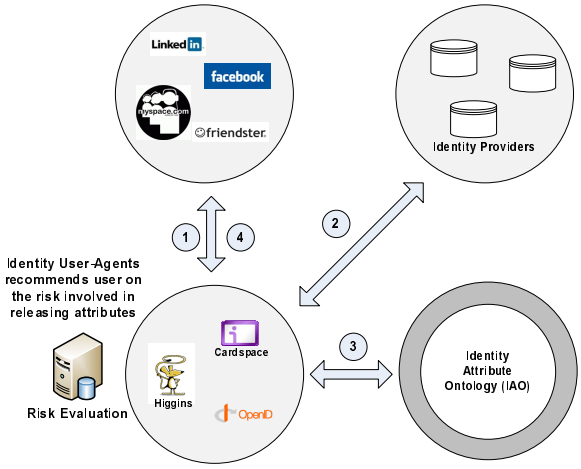


Fig. 2. Risk Evaluation in User-Centric DIM

are shown as numbers of the form $[r_f : r_p]$. Also, composite classes are depicted as black circles.

In IAO, it is assumed that each individual belongs to a single class. For an individual *i* belonging to multiple classes, we can insert a virtual class between *i* and these classes, to satisfy the single-class restriction. Also, if some risk values need to be defined on particular individuals, we create a class for such an individual, and let all the risk values be defined on classes.

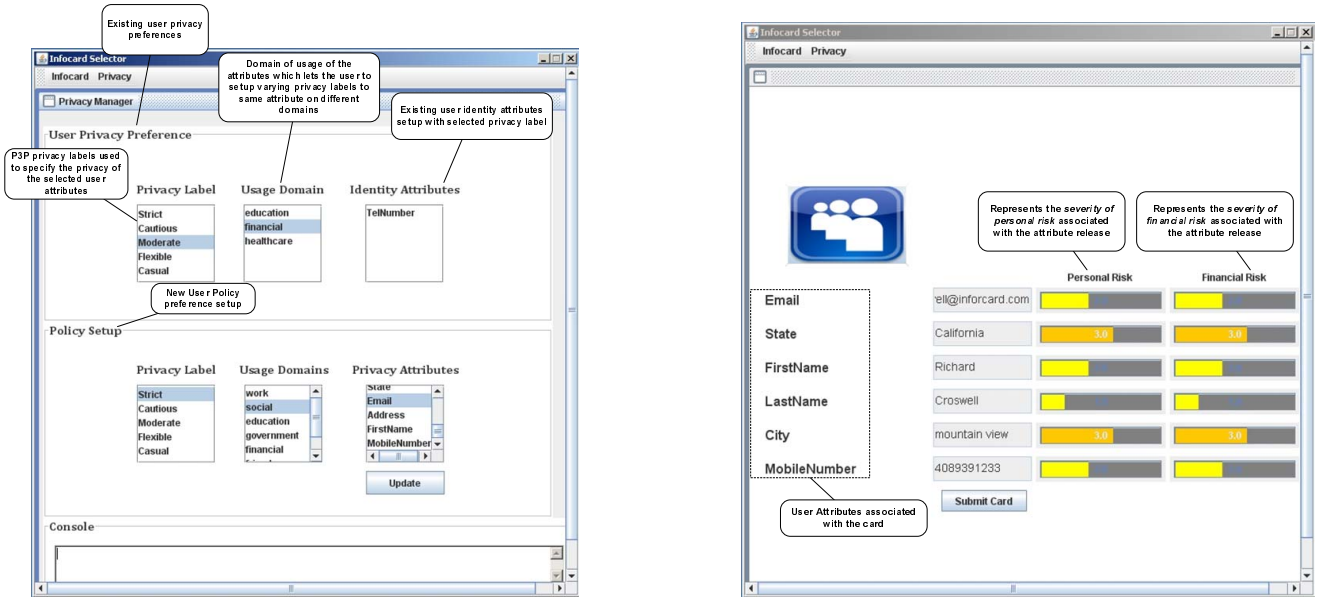
We create a *combination risk class*, which is a composite class connected by *partOf* links from its component classes. The combination risk classes also have a risk value associated with them which depicts the risk involved in the combined release of the component classes. Suppose the class C represents that if *SSN* and *personal-email* are going to be released, then its risk values [3:5] are applied. These values are higher than that of the risk values of the component classes, or it can be interpreted as a suggestion made to the user for not allowing the combined release to avoid possible linkage of these identities. Therefore, a combination risk class will have higher f-risk and p-risk values than that of its component classes.

C. Risk Evaluation

IAO is modeled with generic classes representing the identity information in the OSN. The classes, individuals and combination risk classes are defined to represent the relationship among social network identity attributes. When the user requests a service to SP which requires a certain user identity information, the UA handles the disclosure of *RA* of the SP. Before sending the *RC* and completing the transaction, UA uses IAO to perform risk evaluation which presents the user with the potential risk in releasing the identity information to the SP as shown in Figure 2.

D. User Privacy Preference Evaluation

To ensure privacy of the presented identity attributes, various machine-readable privacy expression languages for the SP [12] are used to express their intents in handling



(a) User Privacy Preference Manager

(b) Risk Evaluation on Identity Attributes

Fig. 3. Identity Selector Tool

identity attributes. The main goal of this standardized policy languages allows the UA to interpret the SP's privacy policies and determine the privacy violations based on the user's privacy preferences on their identity attributes. Though the risk evaluation is based on a generic IAO, the privacy violation evaluation [2] provides the SP with specific violations for the identity disclosure as illustrated in Algorithm 1.

Algorithm 1: Evaluate Privacy

Require: $domain$, $attribute$, $privacylabel$
  load user privacy preference db as $userdb$
  if $domain \in userdb$ **then**
    get all the $existing\ policy$ for $domain$
    if $\exists$ conflicts in $existing\ policy$ **then**
      prompt user with policy violation
    else if $attribute \notin existing\ policy$ **then**
      prompt user with non-existent policy
    else
      return true
    end if
  else
    prompt user to setup policy
  end if

IV. Implementation Details

Our implementation is based on the development of extension modules for an existing user-centric card-based identity selector tool [3]. The identity selector tool is a java-based implementation consisting of UA which supports locally-stored personal cards and IdP-stored managed cards. We enhanced the UA to include the privacy preference manager, privacy evaluation engine, and the risk evaluation module using an ontology as a web services. We implemented the above-mentioned modules with (1) Eclipse galileo using java 1.6.0.18, (2) Apache Tomcat Server 6.0.14, (3) Eclipse WTP (Web Tools Platform) 3.5 plug-in, (4) P3PLite Schema for server policies, and (5) Protege java API version 3.0.

Identity Selector in Figure 3 is a java-based user-centric identity management tool which allows the user to securely manage and disclose their identity attributes over the web. User identity attributes are collectively represented as cards which can be selected by the user to disclose certain identities to the SP. It provides the users with an option to manage their card locally as Personal Cards or with an IdP as Managed Cards. IdP, one of the core components of our tool, is also implemented that is used store the user's identity attributes as managed cards. Cryptographic libraries were used to securely store and exchange user identity attributes between core components of the tool.

Privacy preference evaluation provides an interface to manage user privacy preferences on identity attributes based on the OSN domain. As shown in Figure 3(a), user privacy preferences are expressed which are converted from/to *PREP* specifications to support the privacy evaluation.

Risk evaluation is performed on the attributes which ought to be released by the user to the SP. The Identity selector tool generates requests to the IAO web service to calculate the risk values for the user identity attributes. The risk values are represented as a risk bar to emphasize the severity by different colors such as yellow (low risk), orange (medium risk), and red (high risk)[1]. The risk value presentation is depicted in Figure 3(b).

[1]Even though our risk calculation is quantitative-based, the results are presented in a qualitative manner.

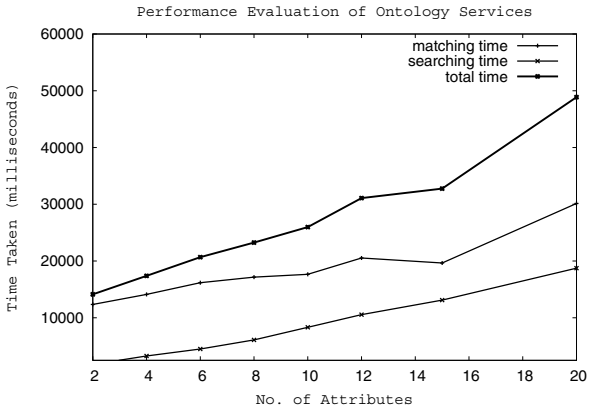


Fig. 4. Performance Evaluation of Ontology Service

IAO implementation and evaluation were realized by adopting the protege API [15] developed by Center for Biomedical Informatics Research at Stanford University. We modeled the user attributes which represents their persona in various OSNs as an ontology which can provide a hierarchical relationship among those attributes. We identified four popular SPs which play a vital role in the area of information sharing between friends and relations, professionals and college students social network which can emulate the requirement for multiple persona for a user. These identity attributes are collected from existing social networks including Linkedin, Facebook, MySpace and Friendster to build the ontology. The semantic similarity matching algorithms proposed in [9] are also adopted and the IAO is published as a *SOA*-based web services to support a dynamic and distributed nature of DIM.

For our evaluation as in Figure 4, we have identified various checkpoints in the ontology service request. We have mainly considered the matching (x ms) and searching (y ms) functions as two critical checkpoints and observed their performances. Though the ontology service takes a considerable time to load the existing ontology classes for each request, this can be optimized by caching them rather than re-performing the same operation for every request. Figure 4 shows that the total time taken for our evaluation has a linear increase and the web services-based ontology was a promising solution for any open identity solution with the improved user-centricity.

V. Conclusion

We have proposed an ontology-based user-centric DIM to perform risk evaluation for user identity attributes which would be disclosed to various SPs by the user. We have also introduced a domain-based privacy preference evaluation with respect to the SP's privacy policies, especially for the OSN environment which enables the user to specify fine-grained user privacy policies to preserve their privacy at the SP. We have also presented the implementation results of the proposed mechanisms to prove its feasibility and usability. By applying these mechanisms to a dynamic environment such as OSN, we have demonstrated how DIM can reduce the risks involved with identity theft and privacy violations.

The current ontology implementation is extensible to perform dynamic risk evaluation for the user identity attributes based on certain factors such as reputation of the SP or the user disclosure pattern to other similar SPs. This can be achieved using existing mechanisms on reputation systems [17] and identity usage pattern [13]. In order to make the ontology service more dynamic, the UA may need to adopt one of these mechanisms for reflecting the existing risk values of the ontology classes. The reputation system can be built as part of ontology service which collects the peer responses using user feedback or other data mining mechanisms. Tracking user identity usage pattern by the UA can be performed in IAO where the UA frequently updates the risk values of the ontology classes based on the user behavior with various SPs.

Acknowledgments

This work was partially supported by the grants from National Science Foundation, Department of Energy and Open Invention Network.

References

[1] Higgins identity framework. available at `http://www.eclipse.org/higgins/`.

[2] G.J. Ahn, M. Ko, and M. Shehab. Privacy-enhanced User-Centric Identity Management. In *Proceedings of International Conference on Communications*. IEEE, 2009.

[3] G.J. Ahn and J. Lam. Managing privacy preferences for federated identity management. In *Proceedings of the 2005 workshop on Digital identity management*, page 36. ACM, 2005.

[4] L. Alliance. Liberty alliance project. *Web page at http://www. projectliberty. org*.

[5] V. Bertocci, G. Serack, and C. Baker. Understanding windows cardspace: an introduction to the concepts and challenges of digital identities. 2007.

[6] L.F. Cranor, M. Arjula, and P. Guduru. Use of a P3P user agent by early adopters. In *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, pages 1–10. ACM New York, NY, USA, 2002.

[7] L.F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 13(2):178, 2006.

[8] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, page 666. ACM, 2007.

[9] M. Iwaihara, K. Murakami, G.J. Ahn, and M. Yoshikawa. Risk evaluation for personal identity management based on privacy attribute ontology. In *Proceedings of the 27th International Conference on Conceptual Modeling*, page 198. Springer, 2008.

[10] D.N. Jutla and P. Bodorik. Sociotechnical architecture for online privacy. *IEEE Security & Privacy*, pages 29–39, 2005.

[11] L. Kagal, T. Finin, and A. Joshi. A policy based approach to security for the semantic web. *Lecture Notes in Computer Science*, pages 402–418, 2003.

[12] P. Kumaraguru, L. Cranor, J. Lobo, and S. Calo. A survey of privacy policy languages. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, volume 48, 2007.

[13] D. Mashima and M. Ahamad. Towards a User-Centric Identity-Usage Monitoring System. *Proc. of ICIMP*, 2008, 2008.

[14] D.L. McGuinness, F. Van Harmelen, et al. OWL web ontology language overview. *W3C recommendation*, 10:2004–03, 2004.

[15] N.F. Noy, M. Sintek, S. Decker, M. Crubézy, R.W. Fergerson, and M.A. Musen. Creating semantic web contents with protege-2000. *IEEE Intelligent Systems*, 16(2):60–71, 2001.

[16] D. Recordon and D. Reed. OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, page 16. ACM, 2006.

[17] G. Zacharia and P. Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9):881–907, 2000.