Privacy and Reputation in Context Aware e-Learning

R. Jayashree
Assistant Professor,
Dept of IT, SRM /University, Chennai, India.

A. Christy, Ph.D
Principal, St.Mary's School of Management,
Sathyabama University, City, Chennai, India.

ABSTRACT

Contextualization is a paradigm for building intelligent systems that can better predict and anticipate the needs of users, and act more efficiently in response to their behaviour. Privacy and legal protection rights are a major challenge that needs to be tackled when capturing and using contextual data for recommendation. The privacy of learners can be protected through identity management. Participants can hold multiple identities or can adopt new pseudonymous personas. A pseudonymous actor needs a privacy-preserving mechanism for the transfer or merger of their reputation across their multiple pseudonyms. A reliable and trustworthy mechanism for reputation transfer (RT) from one persona to another is required. Such a reputation transfer model must preserve privacy and prevent link ability of learners' identities and personas. In this paper, we present an identity management-based solution to privacy and a privacy-preserving reputation management (RM) system which allows secure transfer of reputation. This paper includes the online rating calculation method for reputation management.

General Terms

Adaptive and intelligent educational systems, identity management, reputation management.

Keywords

Reputation-Ranking method, Ranking using Bayesian Approximation, Trust and Reputation Relationship.

1. INTRODUCTION

One of the most cited definitions of context is the definition of Dey et al. [2] that defines context as "any information that can be used to characterize the situation of an entity. An entity is person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves. "Pioneering work on context-aware recommender systems has been done by Adomavicius and Tuzhilin [3]. The authors researched approaches where the traditional user/item paradigm was extended to support additional dimensions capturing the context in which recommendations are made.Privacy and legal protection rights are a major challenge that needs to be tackled when capturing and using contextual data for recommendation. So far, researchers have often ignored privacy issues. However, if context aware recommender technologies want to move beyond the current prototype phase, practical solutions regarding legal and privacy issues are needed. The challenge needs to be tackled from two perspectives are the privacy of the target users' needs to be preserved in order to deploy current prototypes in real-life settings and the sharing and exchange of data is a key requirement to enable comparative evaluation studies. Trust relationships among co-learners are important for collaboration activities in e-learning environments. A trust relationship may need to be developed between two unknown learners who find themselves working together. In a trust relationship, an individual's requirement for privacy may be diminished by expectations of trust or an individual may forfeit privacy to gain trust [13]. Privacy risk is minimized when a trust-based disclosure decision is made. However, misplaced trust results severe threats to privacy. Privacy and trust are equally desirable in a learning environment. Privacy promotes safe learning, while trust promotes collaboration and healthy competition, and thereby, knowledge dissemination.

Reputation appears to be one effective source for measuring trust. Reputation is a contextual and longitudinal social evaluation on a person's actions [13]. An e-learning environment may bring the possibly pseudonymous users together through chat, message board, threaded discussion, online conferencing, email, blogs, etc. Research has shown that it is both unnecessary and privacy threatening to divulge a user's real identity in most online-learning related activities [14], [15]. Therefore, the trustworthiness of a pseudonymous entity needs to be estimated without the full Knowledge of a real-world identity [13].Identity management (IM) has been shown to offer an effective solution to privacy [3], particularly in the learning domains [14], [15]. In such a privacy-enhancing identity management scheme, each user participates in a context by assuming a context-specific partial identity and potentially many different identifiers or pseudonyms. Besides for privacy reason, learners may use multiple identities in open learning environments (e.g., OpenLearn) for different learning purposes. The trustworthiness of a pseudonymous user can be computed by measuring reputation on various aspects of trust pertinent to the underlying context. However, a proper reputation assessment is disrupted when an individual acts under multiple partial identities [13]. Trust is essential to successful collaboration among learners [17], [18]. Online collaboration can cause stress depending on the level of the collaborators' mutual trust [19]. In a learning environment, various key relationships of recommender-recommendation seeker, peer-peer, helper-helpee, and mentor-mentee are formed based on mutual trust [13].Privacy concerns are inherent in a collaborative environment. The privacy concerns in collaborative systems originate from individuals' desire to control how one is perceived by another [20].

In this paper, we first present an analysis of privacy challenges for the development and evaluation of context aware recommender systems for learning that are able to generate recommendations adapted to the current contextual needs of the user. Second, trust and privacy relationship is built with reputation management (RM) system. Third, RM method, ranking are discussed.

This paper is organized as follows. Section 2 describes related work. Section 3 describes privacy challenges in context-aware recommender systems. Section 4 discusses relationships between trust, privacy and reputation management. In Section 5, we present reputation ranking method using bayesian approximation. Section 6 concludes and describes future work.

2. MOTICATION AND BACKGROUND

Several contextual recommender systems have been developed that use paradigms in various application domains. Examples include context-aware recommender systems that suggest gas stations to a driver of a car [5], contextualized media delivery systems [4], [6] and intelligent tourist guides [3]. For example, COMPASS [7] is a recommender system that uses a context-driven querying and search approach to provide a tourist with information about nearby monuments, hotels and people. In an evaluation experiment, time and location were used to contextualize recommendations. Interestingly, the authors report that "last time visited" had a negative influence on the perceived usefulness of the system. These results illustrate that careful analysis of data that is taken into account is necessary when deploying contextualization algorithms. Adomavicius and Tuzhilin [3] identify the development of high-performing context-aware recommender systems and testing them on practical applications as an important challenge. They argue that most work on context-aware recommender systems has been conceptual, where a certain method has been developed, tested on some (often limited) data, and shown to perform well in comparison to certain benchmarks. Among others, they argue that there has been little work done on developing novel data structures and new system architectures for CARS that incorporate context sensors and various filters and converters in a modular fashion. A third important challenge is the evaluation and lack of publicly available datasets [3], [8]. In order to assess the impact of various contextual parameters, data sets are needed that contain contextual data.

The challenges outlined above are explored for the development of CARS for learning is defined [1]. Katrien Verbert et al.[1] have presented a survey of context-aware recommender systems that have been deployed in TEL settings. The expectations of trust and privacy among the users of e-learning systems affect learning activities and learning outcomes. An approach to address privacy protection and trust facilitation is explored [13]. Reputation is an effective means to measure trust in e-learning environments. A mechanism to evaluate and attach reputation to a pseudonymous identity can help measure trust without the loss of privacy [13].Reputation management can help attach a reputation marker to an anonymous or pseudonymous identity and thereby facilitate trust. Since users need to assume multiple non-linkable partial identities to protect their privacy, there is a need for reputation transfer among the partial identities [13]. Privacy protection in reputation transfer requires that the transfer must occur without letting anyone easily observe such a transfer or be able to link two partial identities querying reputation. Besides, reputation is contextual and needs to be assessed within a context for accuracy [13].

Mohd Anwar and Jim Greer [13] has developed a solution and implemented by which privacy preserving and contextual reputation assessment can be done with the aid of a trusted guarantor. Mohd Anwar and Jim Greersolution has limitationsand cannot be applied in other domains like-business, where both privacy and trust are important. Mohd Anwar and Jim Greerwork can be expanded to facilitate reputation-based trust while supporting privacy-preserving identity management in online communities. In the privacy trust tradeoff issues, a user may choose to trade their privacy for a corresponding gain in their partner's trust. In an asymmetric trust relationship, the weaker party must trade this privacy loss for a trust gain, which is required to start interaction with the stronger party [21]. Mohd Anwar and Jim Greer [13] approach offers mechanisms for restricting linkability of partial identities. The limitation of this approach is that if an attacker continuously changes the ratings she assigns to various identities and observes the results for a long time, then the attacker might be able to link identities. However, unlike a financial institution, stakes of doing so is low in a learning environment. Furthermore, we believe that he guarantor can address these attacks through routine auditing and proper mediation.

This paper supports privacy while facilitating reputation-based trust. Marsh addresses the issue of formalizing trust as a computational concept in his PhD dissertation [27]. In his model, trust is treated as a subjective and mathematical entity, and it is computed using a subjective real number arbitrarily ranging from -1 to +1. In the work of Golbeck and Hendler, trust is treated as a measure of uncertainty in a person or a resource [28]. Specifically, they suggested an algorithm for inferring trust by polling ratings from one's trusted neighbors in a social network. In both of the models [27], [28], reputation is synonymous with the measure of trust. We use reputation to measure trust for e-learning.

3. PRIVACY CHALLENGES IN CONTEXT-AWARE RECOMMENDER SYSTEMS

Privacy and legal protection rights are a major challenge that needs to be tackled when capturing and using contextual data for recommendation. The privacy of the target users' needs to be preserved in order to deploy current prototypes in real-life settings and the sharing and exchange of data is a key requirement to enable comparative evaluation studies. Privacy rights of the target users must not get harm and are willing to make scientific data available. They are missing a condensed overview of the legal situation and practical solutions regarding data set sharing. Guidelines are developed that document data protection laws like the European Directive on data protection 95/46/EC [10]. The main principles of this directive have been discussed in [11]. Users must be made aware of what data is being gathered and what it is being used for. Users should be given information, access, and control over data, and data has to be stored securely. Several frameworks to address these requirements are discussed in the literature [12], [13].

4. RELATIONSHIPS BETWEEN TRUST, PRIVACY AND REPUTATION MANAGEMENT

Trust and privacy are interrelated constructs—disclosure of personal information depends on trust [23]. Since trust reduces the perceived risks involved in revealing private information, it is a precondition for self-disclosure [24]. On the other hand, trust invokes the threat of privacy violation, identity theft, and threat to personal reputation [24]. In policy-based trust, privacy loss from credential disclosure is addressed through trust negotiation [25]. Trust is gained when there is a loss in privacy. The Fig.1 shows the relationship between privacy and trust.

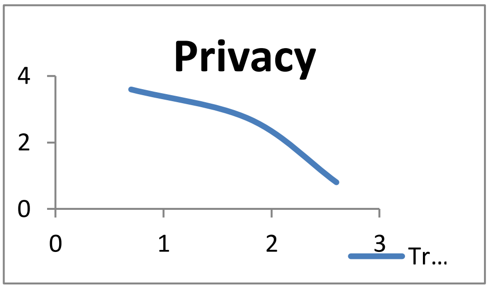

Fig.1

Privacy awareness becomes very important in a collaborative environment. The primary desire for privacy control in collaborative work settings comes from the desire of "impression management" [20]. Furthermore, since high reputation creates positive impression about a user, we take the view that reputation management also contributes to "impression management." Individuals with good reputation are usually trusted and valued in a relationship. Two scenarios of transfer or merger of partial identities are:

1) A user requests transfer or merger and the system obliges with the mediation of a guarantor,

2) The system automatically performs transfer or merger based on the decision of the guarantor.

Reputation earned on any partial identity is merged with reputation of all other partial identities of a user within the same context. Unfortunately, a privacy concern is inherent in reputation transfer. Observing a transfer of reputation from one identity to another, an observer can easily link two identities involved in the reputation transfer, failing an identity-management-based solution [15] to privacy. Therefore, a pseudonymous actor needs a privacy-preserving mechanism for the transfer or merger of their reputation across their multiple pseudonyms. Privacy awareness becomes very important in a collaborative environment. The primary desire for privacy control in collaborative work settings comes from the desire of "impression management" [20]. Privacy in the form of anonymity could diminish trust. List of dimension-relevant features is presented to a rater to capture the rater's opinion along the respective trust dimension. Features are qualities of learners desirable in learning activities. Reputation of an identity for a specific dimension is estimated. A pseudonymous actor needs a privacy-preserving mechanism for the transfer or merger of their reputation across their multiple pseudonyms. Privacy protection in reputation transfer further requires that the transfer must occur without letting anyone recognize such a transfer. In the RT model, non-observable and non-linkable reputation transfer is done.

Partial identity attributes may include information about reputation earned over their behavior (Fig. 2). An advantage of carrying reputation with identity is that it allows an individual to establish a trust relationship fairly easily. This reputation can be transferred or merged and thus observer views the total or modified reputation. Trust can be seen as a complex predictor of an entity's future behavior based on past behavior. In our daily life, we always deliberate whether we could trust someone with something. Likewise, it is also crucial to calculate the trustworthiness of a user to decide what piece of information would be safe with whom and in what context. People are not likely to reveal confidential information about themselves to an untrustworthy party. Trust plays a major role in reducing privacy concerns.

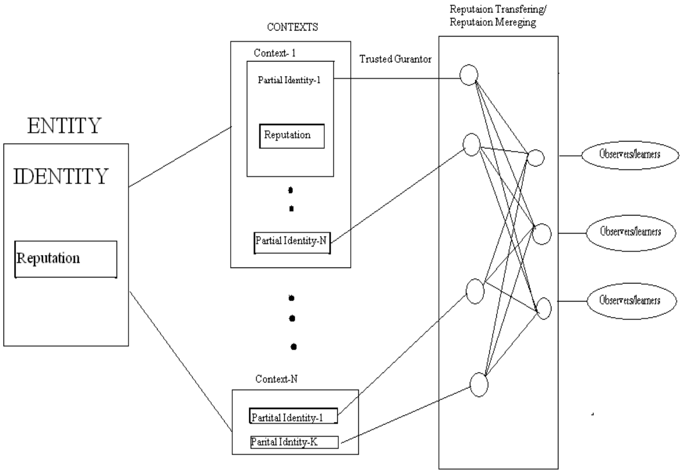

Fig.2

5. REPUTATION AND RANKING

This section discusses approximation techniques for Bayesian inference.

5.1 A Bayesian Approximation Method for Online Ranking

Given the total reputation of k pseudonyms, we define r(i) as the rank of entity i. If pseudonym's identity $i_1, \ldots, i_d$ are tied together, we have $r(i_1) = \ldots = r(i_d)$ and let the entity q ranked next have $r(q) = r(i_1) + d$

Table 1. Notation Explanation

K	- number of entities
N*i*	- number of pseudonym identities for entity i
Θ_{ij}	- strength(reputation) of the jth partital identity for entity i
$N(\mu_{ij}, \sigma^2_{ij})$	- prior distribution of Θ_{ij}
Z_{ij}	- standardized quantity of Θ_{ij}
Θ_i	- strength of entity i; $\Theta_i = \Sigma\ \Theta_{ij}$
β^2_i	- uncertainty about the performance of entity i
X_i	- performance of entity i ($X_i \sim N(\Theta_i, \beta^2_i)$ for Thurstone-Mosteller model)
$N(\mu_i, \sigma^2_i)$	- prior distribution of Θ_i
Z_i	- standardized quantity of Θ_i
ϕ	- probability density function of a standard normal distribution
ϕ	- cumulative distribution function of a standard normal distribution
ϕk	- probability density function of a k-variance standard normal distribution
ϕk	- cumulative distribution function of a k-variate standard normal distribution

ƙ - a small positive value to avoid σ2i becoming negative

D - the overall reputation

From a Bayesian perspective, both the observed data and the model parameters are considered random quantities. Let D denote the observed data, and Ɵ the unknown quantities of interest. The joint distribution of D and Ɵ is determined by the prior distribution P(Ɵ) and the likelihood P(D\Ɵ):

$$P(D,\Theta) = P(D\backslash\Theta)P(\Theta)$$

After observing D, Bayes theorem gives the distribution of Ɵ conditional on D:

$$P(\Theta\backslash D) = P(\Theta,D)/P(D)$$

$$= P(\Theta,D)/\int P(\Theta,D)d\Theta$$

This is the posterior distribution of Ɵ, which is useful for estimation. Quantities about the posterior distribution such as moments, unities, etc., can be expressed in terms of posterior expectations of some functions g(Ɵ); that is,

$$E[g(\Theta)\backslash D] = \int g(\Theta)P(\Theta,D)d\Theta \,/\, P(\Theta,D)d\Theta$$

The probability P(D), called evidence or marginal likelihood of the data, is useful for model selection. Both P(Ɵ\D) and P(D) are major objects of Bayesian inference.

5.2 Approximating the Expectations

Let Θ_i be the reputation value of entity i whose ability is to be estimated. Bayesian online rating systems start by assuming that Θ_i has a prior distribution $N(\mu_i,\sigma^2_i)$ with µi and σ^2_i known, next model the reputation-ranking outcome by some probability models, and then update the skill (by either analytic or numerical approximations of the posterior mean and variance of Θ_i) at the end of the overall reputation-ranking calculation. These revised mean and variance are considered as prior information for the next reputation value, and the updating procedure is repeated.

To start, suppose that entity i has a reputation value Θ_i and assume that the prior distribution of Θ_i is $N(\mu_i, \sigma^2_i)$.

Upon the completion of a reputation-ranking calculation, their skills are characterized by the posterior mean and variance of $\Theta = [\Theta_1,\dots, \Theta_k]^T$.

Let D denote the result of a reputation-ranking calculation and $Z = [Z_1,\dots,Z_k]^T$ with

$$Z_i = (\Theta_i\text{-}\ \mu_i) / \sigma_i,\ \ i = 1,\dots, k,$$

where k is the number of entities. The posterior density of Z given the reputation-ranking outcome D is

$$P(z\backslash D) = C\phi k(z)f(z),$$

where f(z) is the probability of reputation-ranking outcome P(D\z).

6. CONCLUSION AND FUTURE WORK

Reputation is an effective means to measure trust in e-learning environments. A mechanism to evaluate and attach reputation to a pseudonymous identity can help measure trust without the loss of privacy. Reputation management can help attach a reputation marker to an anonymous or pseudonymous identity and thereby facilitate trust. Since users need to assume multiple non linkable partial identities to protect their privacy, there is a need for reputation transfer among the partial identities. Privacy protection in reputation transfer requires that the transfer must occur without letting anyone easily observe such a transfer or be able to link two partial identities querying reputation. Besides, reputation is contextual and needs to be assessed within a context for accuracy. A solution has been developed and implemented by which privacy preserving and contextual reputation assessment can be done with the aid of a trusted guarantor. The system can help learners to successfully identify potentially good helpers or collaborators. The expectations of trust and privacy among the users of e-learning systems affect learning activities and learning outcomes. This paper is to help learners to successfully identify trusted helper or collaborators.

In this paper, reputation management for privacy and collaborative learning is explored. Reputation is an effective means to measure trust in e-learning environments. A mechanism to evaluate and attach reputation to a pseudonymous identity can help measure trust without the loss of privacy. A solution has been developed and implemented by which reputation transferring and/or merging can be done with the aid of a trusted guarantor. In summary, this paper approximates the expectation of entities' performances to derive simple update rules for online ranking using bayesian approximation method. The proposed method is efficient and can be easily applied to large-scale systems with multiple entities and multiple pseudonym identities.

6.1 Future Work

A user may choose to trade their privacy for a corresponding gain in their partner's trust. In an asymmetric trust relationship, the weaker party must trade this privacy loss for a trust gain, which is required to start interaction with the stronger party. In future work, different RT methods will be analysed and compared. This paper presents the relationship between trust and privacy and in future we are planning to explore the how much amount of privacy loss is needed to gain trust from the learners. Learners can also be categorized based on their context and intelligence. In future we decided to find how this categorization affects the reputation and trust values.

7. ACKNOWLEDGMENTS

The author, Jayashree. R, like to thank Dr. Venkatesh. S for his support during the initial phase of the work.

8. REFERENCES

[1] Katrien Verbert, Member, Nikos Manouselis, Xavier Ochoa, Martin Wolpers, Hendrik Drachsler, Ivana Bosnic, and Erik Duval, "Context-Aware Recommender Systems for Learning: A Survey and Future Challenges," IEEE Transaction on Learning technologies, Vol. 5, No. 4, Oct-Dec 2012.

[2] Dey, G. Abowd, and D. Salber, "A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications," HumAN-Computer Interaction, vol. 16, pp. 97-166, Dec. 2001.

[3] G. Adomavicius and A. Tuzhilin, "Context-Aware Recommender Systems," Recommender Systems Handbook: A Complete Guide for Research Scientists and Practitioners, L. Rokach, B. Shapira, P. Kantor, and F. Ricci, eds., pp. 217-250, Springer, 2011.

[4] Z. Yu, X. Zhou, D. Zhang, C.-Y. Chin, X. Wang, and J. Men, "Supporting Context-Aware Media

Recommendations for Smart Phones," IEEE Pervasive Computing, vol. 5, no. 3, pp. 68-75, July- Sept. 2006.

[5] [5] R. Bader, E. Neufeld, W. Woerndl, and V. Prinz, "Context-Aware POI Recommendations in an Automotive Scenario Using Multi- Criteria Decision Making Methods," Proc. Workshop Context- Awareness in Retrieval and Recommendation, pp. 23-30, 2011.

[6] H.-S. Park, J.-O. Yoo, and S.-B. Cho, "A Context-Aware Music Recommendation System Using Fuzzy Bayesian Networks with Utility Theory," Fuzzy Systems and Knowledge Discovery, L. Wang, L. Jiao, G. Shi, X. Li, and J. Liu, eds., vol. 4223, pp. 970-979, Springer, 2006.

[7] M. Van Setten, S. Pokraev, and J. Koolwaaij, "Context-aware Recommendations in the Mobile Tourist Application COMPASS," Adaptive Hypermedia and Adaptive Web Based Systems, pp. 235-244, Aug. 2004.

[8] Z. Yujie and W. Licai, "Some Challenges for Context-aware Recommender Systems," Proc. Fifth Int'l Conf. Computer Science and Education (ICCSE), pp. 362-365, 2010.

[9] G. Adomavicius, A. Tuzhilin, and E.W. Luca, "Context-Awareness in Recommender Systems: Research Workshop and Movie Recommendation Challenge Categories and Subject Descriptors," Human Factors, pp. 60558-60558, 2010.

[10] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Official J. L 281 of 23.11.1995, pp. 31-39.

[11] P. Lonsdale, C. Barber, M. Sharples, and T.N. Arvantis, "A Context-Awareness Architecture for Facilitating Mobile Learning," Learning with Mobile Devices Research and Development, J. Attewell and C. Savil-Smith, eds., pp. 79-85, Learning and Skills Development Agency, 2004.

[12] S. Gurses and R. Vuorikari, "Privacy Issues and Data Protection in Technology Enhanced Learning," Proc. First Workshop Data Sets for Technology Enhanced Learning, http://homes.esat.kuleuven.be/~sguerses/talks.html, 2011.

[13] Mohd Anwar and Jim Greer. "Facilitating Trust in Privacy-Preserving E-Learning Environments," IEEE Transaction on Learning technologies, VOL. 5, NO. 1, JAN-MAR 2012.

[14] M. Anwar, J. Greer, and C. Brooks, "Privacy Enhanced Personalization in E-Learning," Proc. Int'l Conf. Privacy, Security, and Trust, 2006.

[15] K. Borcea, H. Donker, E. Franz, A. Pfitzmann, and H. Wahrig, "Towards Privacy-Aware eLearning," Proc. Privacy Enhancing Technologies, pp. 167-178, 2005.

[16] R.E. Leenes, "User-Centric Identity Management as an Indispensable Tool for Privacy Protection," Int'l J. Intellectual Property Management, vol. 2, no. 4, pp. 345-371, 2008.

[17] J. Mason and P. Lefrere, "Trust, Collaboration, and Organisational Transformation," Int'l J. Training and Development, vol. 7, no. 4, pp. 259-271, 2003.

[18] C. Haythornthwaite, "Facilitating Collaboration in Online Learning," J. Asynchronous Learning Networks, vol. 10, no. 1, pp. 7-23, 2006.

[19] J. Allan and N. Lawless, "Stress Caused by Online Collaboration in E-learning: A Developing Model," Education and Training, vol. 45, nos. 8/9, pp. 564-572, 2003.

[20] S. Patil and A. Kobsa, "Privacy in Collaboration: Managing Impression," Proc. First Int'l Conf. Online Communities and Social Computing, 2005.

[21] L. Lilien and B.K. Bhargava, "A Scheme for Privacy-preserving Data Dissemination," IEEE Trans. Systems, Man, and Cybernetics, vol. 36, no. 3, pp. 503-506, May 2006.

[22] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and Identity Management," IEEE Security and Privacy, vol. 6, no. 2, pp. 38-45, Mar./Apr. 2008.

[23] P. Briggs, B. Simpson, and A.D. Angeli, "Personalisation and Trust: A Reciprocal Relationship?" Designing Personalized User Experiences in eCommerce, pp. 39-55, Kluwer Academic, 2004.

[24] J.L. Steel, "Interpersonal Correlates of Trust and Self-Disclosure," Psychological Reports, vol. 68, pp. 1319-1320, 1991 B. Friedman, P.H. Kahn Jr., and D.C. Howe, "Trust Online," Comm. ACM, vol. 43, no. 12, pp. 34-40, 2000.

[25] W. Nejdl, D. Olmedilla, and M. Winslett, "Peertrust: Automated Trust Negotiation for Peers on the Semantic Web," Proc. 30th Workshop Secure Data Management in a Connected World (SDM '04), pp. 118-132, 2004.

[26] T. Yu and M. Winslett, "Policy Migration for Sensitive Credentials in Trust Negotiation," Proc. ACM Workshop Privacy in the Electronic

[27] Soc. (WPES '03), pp. 9-20, 2003. [27] S. Marsh, "Formalising Trust as a Computational Concept," PhD dissertation, Univ. of Stirling, 1994.

[28] [28] J. Golbeck and J. Hendler, "Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-Based Social Networks," Proc. Eng. Knowledge in the Age of the SemanticWeb, 2004.

[29] Thomson Reuters, "The World University Rankings," http://www.timeshighereducation.co.uk/world-university-rankings/2012-13/world-ranking