A Privacy-Preserving Reputation Management System in E-Learning

J.Ramya Beaula, M.E.,
ramya.jeyaraj@yahoo.co.in

***Abstract*—This research explores a new model for facilitating trust in online e-learning. The privacy of learners is protected through identity management system, where personal information are protected through some degree of participant anonymity or pseudonymity. In order to expect the learners to trust other pseudonymous participants, it is realized that a reliable mechanism is needed for managing participants' reputations and assuring that such reputations are legitimately obtained. Further, since participants can hold multiple identities or can adopt new pseudonymous personas, a reliable and a trustworthy mechanism for reputation transfer from one persona to another is required. Obviously such a reputation transfer model must preserve privacy and at the same time prevent link-ability of learners' identities and personas. In this paper a privacy-preserving reputation management system is presented which allows secure transfer of reputation. A prototypical implementation of the reputation transfer protocol and the successful experimental deployment of the reputation management solution in an e-learning discussion forum serve as a proof of concept.**

***Index Terms*—e-Learning Environments, Trust, Reputation, Reputation Management, Identity Management, Privacy.**

I. Introduction

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. The meaning of trust differs from one context to another. The paper deals with this aspect of trust. Therefore, to engage in and maintain a trust relationship, users need to do two things: (i) assess the trustworthiness of the counterpart, (ii) act according to the degree of trustworthiness expected of each other. 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. In traditional face-to-face academic settings, trust is developed through day-to-day activities where everyone gets to see each other on a regular basis and thus grows to know one another. By contrast, 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. Therefore the trustworthiness of a pseudonymous entity needs to be estimated without the full knowledge of a real-world identity. We investigate how reputation can effectively be used as a predictor of a pseudonymous user's future behavior, which is actually a prediction of trustworthiness.

Identity management (IM) has been shown to offer an effective solution to privacy, particularly in the learning domains. 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. Since the partial identities and pseudonyms offered by the privacy-enhancing identity management solutions are not linkable, the complete assessment of reputation can easily be disrupted by switching and shedding of pseudonyms: reputation earned over a pseudonym is unusable with the shedding of that pseudonym or switching to another pseudonym.

This paper is about building a privacy-preserving reputation management system that performs two major reputation assessment tasks: (1) contextual (i.e., partial identity-based) reputation assessment and (2) reputation transfer across and merger among partial identities so as to support comprehensive assessment of reputation. The crux of privacy preservation lies in ensuring that task (2) maintains non-linkability of partial identities. In other words, reputation transfer or merger process should not allow an observer to link partial identities involved in the process. As a result, the presented system measures trust while supporting an identity-management based solution to privacy. Our contributions are as follows:

1) Relationship between Identity

Management and Reputation Management.

We define reputation as a component of an identity, and consequently, we establish the relationship between identity management (IM)and reputation management (RM).

2) *Reputation Assessment in Learning Environments.*

We propose a contextual reputation assessment technique within a learning environment.

3) *Supporting Trust while Preserving Privacy.*

We face the challenge of supporting trust while preserving privacy, and devise a privacy-preserving reputation management solution to address this challenge.

4) *Implementation.*

As a proof of concept, we implement and evaluate our solution in an online learning environment.

II. SUPPORTING TRUST IN LEARNING ENVIRONMENTS

Trust is contextual, and trustworthiness (measured by reputation) is assessed against an identity. We propose that **user-to user trust**, during collaborative learning activities, be realized in two forms: **trust about a purpose** and **trust in a partner** (partner's identity) for which the partner's trustworthiness needs to be assessed.

1) Trust about Purpose**:** In e-learning, each context explicitly or implicitly manifests some purpose for its participants. For example, a math discussion forum context may have a purpose of offering peer tutoring in math. Within the math forum context, there could be more granular contexts like an Algebra thread or Calculus thread for the purpose of peer-tutoring the respective topics. This form of trust is based on the expectation from the purpose of a context.

2) **Trust in Partner:** This form of trust considers the trustworthiness of a partner in a given context. Trust in partners may need further consideration of the roles of, and relationships with, the transacting partners. Some roles convey more trust than others. For example, an instructor role may convey a higher degree of trust. However, not all instructors are equally trusted by learners. A learner may trust one instructor over another based on their perceived relationship or reputation.

III. REPUTATION MANAGEMENT

Due to the observed relationship of identity and reputation management, we offer a standard mechanism for reputation assessment across partial identities. As a result, reputation management involves reputation assessment and reputation transfer or merger.

A. *Reputation Assessment*

We implemented a mechanism for reputation assessment for an actor along the dimensions of competence, benevolence, and integrity. What a particular dimension represents in a given context is specified through a list of features. A list of dimension-relevant features are presented to a rater to capture the rater's opinion along the respective trust dimension. Each feature carries certain weight (strength), according to which it contributes to the relevant dimension. Each rating contributes to the overall reputation of the poster. Finally ,the weighted sum of all the relevant ratings is averaged to calculate reputation along a respective dimension.

The three dimensions of reputation are calculated on the following features: insightful, timely, informative, well written, constructive, and relevant. These features are qualities of learners desirable in learning activities. A user may define a dimension of trust on their own by choosing a list of features and/or their respective weights for measuring a specific dimension of reputation.

B. *Reputation Transfer across Pseudonyms*

With the persistent use of a pseudonym (a partial identity), the attribution of reputation markers to the pseudonym takes place. A pseudonymous user cannot, on their own, transfer or merge reputation across their multiple pseudonyms, yet such ability is highly desirable .Let us consider scenarios from an e-learning discussion forum where users can participate using individual identity or group identity. With a group identity, all the members of the group are represented.

Ratings on a posting made by a user using a group identity should contribute to the reputation of that group identity as well as to the reputation of the group member's(poster's) individual identities. This is a trivial example of a need for reputation transfer from a group identity to an individual identity. Let us consider another scenario from the e-learning context, where an identity expires and reputation from the expired identity needs to be transferred to an existing identity. Anwar & Greer observed that contexts in thee-learning domain are hierarchical and proposed the notion of contextual identity . As a context expires, the reputation of an identity under that context may need to be propagated back to its parent context resulting in a backward propagation of reputation (reputation transfer) from the innermost context to the outermost context.

There is another variation of reputation transfer, which we call reputation merger. It is a process where reputation of two partial identities are updated by each other or aggregated to reputation of a new partial identity. A reputation merger can be viewed as a two-way reputation transfer between two identities or two one-way transfer between each of the identities and a new third identity, which is the case when two partial identities are merged into a new partial identity. We anticipate two scenarios of transferor merger: (a) a user requests transfer or merger and the system obliges with the mediation of a guarantor,(b) the system automatically performs transfer or merger based on the decision of the guarantor.

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 to privacy. Therefore, a pseudonymous actor needs a privacy preserving mechanism for the transfer or merger of their reputation across their multiple pseudonyms. Such a mechanism has three objectives: (i) provide cryptographically secure reputation transfer protocol, (ii) restrict Bad Acting, and (iii) restrict link-ability of partial identities.

C. *A Proof-of-concept Implementation*

The prototypical system incorporating the RT model has been implemented through a client (for users) and a multi-threaded server (for guarantor) suite written in Java language. The Key Generator entity of the secure reputation transfer protocol is implemented using the RSA key pair generation algorithm provided by Bouncy Castle. The model was implemented using JRE 1.5 and *java.security* and *javax.crypto* APIs. The system manages reputation for 3 different generic roles that are present in an e-learning community: helper, peer, and lurker. The system allows a user to perform any of the following 4 tasks: **register** (i.e., register a pseudonym with a guarantor), **evaluate** (i.e., rate a user), **transfer** (e.g., transfer/merge reputation across pseudonyms), and **query** (e.g., query reputation of a pseudonymous user).

D. *Evaluation*

This section reports on two studies: (a) value of reputation management system in e-learning, and (b) validating the implementation of the RT model. The study (b) was designed to see whether the system facilitates secure reputation transfer/merge across multiple pseudonyms.

IV. Related Work

Trust issues on the web have been around since the inception of the web. Trust is a word that people constantly use to mean different things in different circumstances. In the literature, trust is identified in different forms relating to: whether access is being provided to the trustor's resources, the trustee is providing a service, trust concerns authentication, or trust is being delegated . Even though all the stated forms of trust may take place in e-learning, our work mainly targets on user-to-user trust that relates to the trustee providing services.

V. Conclusion

The expectations of trust and privacy among the users of e-learning systems affect learning activities and the outcomes. A naively constructed privacy-enhanced learning environment offers isolated personal learning spaces, which allow learners to be frustrated, overwhelmed, or dissatisfied sometimes with learning objects or instructors. In this paper, an approach is explored to address privacy protection and trust facilitation. Reputation is an effective means to measure trust in e-learning environments. A mechanism to evaluate and attach a reputation to a pseudonymous identity can help measure trust without the loss of privacy. For example, when Alice participate in a discussion forum, her reputation as a friendly and a knowledgeable user may be all that matters to other participants. Reputation management can help to attach a reputation marker to an anonymous or a pseudonymous identity and thereby facilitates trust.

Since users need to assume multiple non-linkable partial identities to protect their privacy, there is indeed a need for reputation transfer among the partial identities. A privacy protection in reputation transfer requires that the transfer must occur without letting anyone easily observe such a transfer or will be able to link two partial identities querying reputation. Besides, reputation is contextual and this needs to be assessed within a context for accuracy. An exact solution has been developed and implemented by which privacy-preserving and contextual reputation assessment can be done with the aid of a trusted guarantor. This system can help learners to successfully identify potentially good helpers or collaborators.

VI. Future Work

Even though our work is geared towards e-learning, the problem of non-linkability disrupting reputation assessment and vice versa is not peculiar to e-learning. This is a limitation of the identity management-based solution to privacy. Therefore, our solution has many broader applications, and this solution is expected to be applied in other domains like e-business, where both privacy and trust are vital.

In order to better analyze the impact of our system on the users' experience, a plan is executed to conduct a large scale study in an online environment where there is no existing trust relationship among users. Furthermore, when it is looked more deeply into privacy trust trade off issues. A user may choose to trade their privacy for a corresponding gain in their partner's trust. In an asymmetric trust relationship, a weaker party must trade this privacy loss for a trust gain, which is required to start an interaction with the stronger party. For a privacy trust trade-off, we would like to build a heuristic tool that would help users with answers to questions related to various privacy and trust, as follows:

- How much privacy is lost by the user while disclosing the given data?

- How much benefits does the user receive from a particular trust gain?

- How much privacy should the user be willing to sacrifice for a certain amount of trust gain?

References

[1] M. Anwar, J. Greer, and C. Brooks, "Privacy Enhanced Personlization in E-learning," in *Proceedings of the 2006 International Conferenceon Privacy, Security, and Trust*, Markham, Ontario, Canada., 2006.

[2] K. Borcea, H. Donker, E. Franz, A. Pfitzmann, and H. Wahrig, "Towards privacy-aware elearning," in *Privacy Enhancing Technologies*, 2005, pp. 167–178.

[3] R. E. Leenes, "User-centric identity management as an indispensable tool for privacy protection," *International Journal of IntellectualProperty Management*, vol. 2, no. 4, pp. 345–371, 2008.

[4] J. Mason and P. Lefrere, "Trust, Collaboration, and Organisational Transformation," *International Journal of Training and Development*, vol. 7, no. 4, pp. 259–271, 2003.

[5] C. Haythornthwaite, "Facilitating Collaboration in Online Learning," *Journal of Asynchronous Learning Networks*, vol. 10, no. 1, pp. 7–23, 2006.

[6] J. Allan and N. Lawless, "Stress Caused by Online Collaboration in e-Learning: A Developing Model," *Education and Training*, vol. 45, no. 8/9, pp. 564–572, 2003.

[7] S. Patil and A. Kobsa, "Privacy in Collaboration: Managing Impression," in *The First International Conference on Online Communitiesand Social Computing*, 2005.

[8] E. Aimeur, H. Hage, and F. S. M. Onana, "A Framework for Privacy-Preserving E-learning," in *Joint iTrust and PST Conferenceson Privacy, Trust Management and Security*, vol. 238. Springer, 2007, pp. 223–238.

[9] E. T. Bates and L. R. Wiest, "Impact of Personalization of MathematicalWord Problems on Student Performance," *The MathematicsEducator*, vol. 14, no. 2, pp. 17–26, 2004.

[10] A. Kobsa and J. Schreck, "Privacy through pseudonymity in useradaptive systems," *ACM Trans. Internet Technol.*, vol. 3, no. 2, pp.149–183,2003.