Role- and Relationship-Based Identity Management for Private yet Accountable E-Learning

Mohd Anwar and Jim Greer

Abstract In every communicative context, each participant assumes some kind of role and negotiates some type of relationship with their counterparts. In the e-learning domain, the roles (e.g. instructor, learner, marker, administrator, etc.) for participants are well structured and relationships (e.g. one-to-one, one-to-many, hierarchical, etc.) among roles are relatively predictable. This paper proposes role-based and relationship-based identity management in the e-learning domain to enable participants to enjoy a desired amount of privacy and to hold participants accountable for their actions. In this approach, a role-based identity hides an actor in the crowd of actors with same roles, and a relationship-based identity allows an actor to disclose information appropriate for a respective relationship. Moreover, public roles (e.g. instructor in a course, disciplinary committee in a department, etc.) are assigned guarantor privileges to sanction foul acting and to facilitate usage control over disclosed information.

1 INTRODUCTION

Historically, privacy is a relatively minor concern in a close knit group like a learning community, where each participant carries one embodied identity. The bodily presence works as the guarantee of authenticity of a participant, which makes the participant more trustworthy and accountable towards other participants. On the other hand, since the participants in e-learning may not carry their embodied identities, identity thefts, social engineering attacks, or man-in-the-middle attacks

Mohd Anwar
ARIES Laboratory, Computer Science, University of Saskatchewan, Saskatoon, SK, CANADA
e-mail: mohd.anwar@usask.ca

Jim Greer
ARIES Laboratory, Computer Science, University of Saskatchewan, Saskatoon, SK, CANADA
e-mail: jim.greer@usask.ca

are more likely to happen in e-learning environments. Even though privacy issues in e-learning are very different from a traditional classroom [1], classroom-based views about privacy are often extrapolated to e-learning. As a result, actors in an e-learning environment retain little privacy and are susceptible to threats ranging from annoying spam attacks to more serious identity frauds.

The realization that online learning brings together participants with a wide range of goals, attitudes and ethical stances, raises concerns about the safety of participants who fail to protect their privacy. E-learners are becoming more perceptive about the privacy implications of their online activities. Borcea et al. point out that privacy requirements are obviously important for e-learning, since they establish an unbiased environment without prejudice or favoritism [2]. A learner should be able to act under different pseudo-identities or, when possible, anonymously. The separation of activities from identity encourages learners to be unrestricted and allows them to learn without pressure.

For reasons similar to those in other domains, privacy is very valuable in the e-learning domain. Privacy protects learners from being mis-defined and judged out of context [4]. For example, the conversation between two co-learners is less guarded than that of the conversation between a learner and an instructor. It may be inappropriate for an instructor to judge a learner based on the learner's conversation with their co-learners in a discussion forum. Westin identifies the following four functions that privacy performs for us: Personal Autonomy, Emotional Release, Self-Evaluation, and Limited and Protected Communications [10]. We see these functions as equally important for the participants in e-learning. Privacy provides autonomy to learners while a threat to autonomy puts an individual under the control of those who know that individual's secrets. Privacy provides moments of "off stage," when the individual can be tender, angry, irritable, frustrated, or dream-filled. In the learning process, it is natural for a learner to be sometimes frustrated, overwhelmed, or dissatisfied with learning objects or instructors. These moments of "off stage". may emerge in conversations among a group of close friends or in a personal blog. Privacy is essential for carrying on self-evaluation and other reflective activities. Learners should be able to play with their seminal or inchoate ideas and verify them with trusted peers or mentors without fear of being ridiculed. Learners should have opportunities to share confidences and intimacies with their trusted colleagues— a close friend, a graduate supervisor, etc. As in any online domain, concerns for privacy of its participants are growing in the e-learning domain. However, in online learning, little consideration is given to privacy and security. Privacy-related research for the e-learning domain is inadequate, and the majority of approaches aim at addressing only learners' privacy. An e-learning system involves participants of various roles designed to participate in various types of relationships in various contexts, including peer coaches, markers, tutors, and other learning support staff. Therefore, privacy concerns of every participant are important and need to be addressed. In that vein, a role-based or a relationship-based solution can cater to privacy needs for participants of any role or relationship.

Each context explicitly or implicitly manifests some purpose for its participants. Based on the purpose, a participant assumes an appropriate role or engages in a re-

lationship. A role can be defined as an expected behaviour attached to the position of an individual in a community. For example, in a learning community, an individual in a teaching role is expected to set learning objectives, give lectures, evaluate students' performance, etc. Likewise, an individual in a basic learner role is expected to enroll in a course and undertake course related activities like attending lectures, asking questions, participating in course evaluation, etc. A relationship is a specific connection manifested in individualized interaction between two roles. For example, in an advisor-advisee relationship, a teacher engages in personalized communication with a student for guiding the student during their academic career. Or, an individual in a student role may engage in a peer relationship with a lab-partner drawn from individuals of the same role (student) in a specific course context.

In the e-learning domain, the number of contexts including the number of roles and relationship types (among roles) for each context are relatively few, and information sharing needs for each role or relationship can be anticipated. As a result, a role- and relationship-based identity management approach effectively partitions an identity into multiple partial identities for the purpose of various contexts, roles, and relationships. Partitioning of identity contributes to information parsimony which, in turn, contributes to privacy. For example, a graduate student holds multiple partial identities based on the role they play: a student, a tutor, an instructor or a marker. In the context of a course in which a student acts in a teaching role, their student id number may be extraneous information whereas in the context of a course in which that student acts in a registrant role, their employee id may be irrelevant.

In a role-based identity, say "student", each actor sharing this role would be identified only by their role (e.g. SomeStudent). A role-based identity allows a participant to be indistinguishable from the other participants of the same role. A relationship-based identity, on the other hand, has one or more of the actors identifiable by a pseudonym rather than by their true identity (e.g. Student23 or Henry). This allows one participant to hold a privacy-preserving relationship with another participant. Since, in every context, each role-based identity (e.g. SomeStudent) serves an actor's purpose in a specific role (e.g. student), and each relationship-based identity (e.g. Student23) serves an actor's purpose in a specific relationship (e.g. lab-partner), any disclosed information is only associable to an identity during the duration of its pertinent role or relationship. When a piece of information is no longer associable to an identity, in effect, that piece of information expires. For example, student23 may accidentally reveal to his lab-partner Bob that he is diagnosed to have HIV. As soon as Bob's relationship with his lab-partner ends, the lab-partner's relationship-based identity with pseudonym student23 expires and this information is no longer associable to an identity. At that point, Bob only knows that some student of his class has HIV. However, privacy without accountability is counter-productive. When innocuous behaviours or relatively minor offenses of an individual ought to be forgotten, their malicious behaviours or serious offenses ought to be tracked. For that reason, public roles (e.g. instructor in a course, disciplinary committee in a department, etc.) are assigned guarantor privileges to connect pseudonyms with actual identities, to sanction foul acting and to authorize usage control over disclosed information.

2 ROLES, RELATIONSHIPS, AND CONTEXTS IN E-LEARNING ENVIRONMENT

Participants of an e-learning system assume following basic kinds of roles: learner, instructor, instructional support, and administrator. In various contexts, each participants of an e-learning environment engages in the following type of relationships: one-to-one, one-to-many, many-to-many, and hierarchical. In a one-to-one relationship, two participants want to be identifiable to each other and distinguishable from other participants. In a one-to-one relationship, the participants share personal information warranted by the role and purpose of the one-to-one relationship. In a one-to-many relationship, a participant wants to communicate with a group of actors in the same manner. In a one-to-many relationship, for example, an instructor in a course wants to inform all the course registrants about course materials. For this kind of purpose, the entire class usually carries a group identity. A many-to-many relationship can be broken into two one-to-many relationships: in a student-instructor many-to-many relationship, a student enrolls in multiple courses and an instructor teaches multiple courses in a semester. A hierarchical relationship serves to define a hierarchy. For example, a student in a marker role grades other students' work. An instructor working as a department head supervises other instructors.

In e-learning, one context cascades into another more finely-grained context attaching a dimension of direction to a role. The roles acting on the most generic context are omni-directional: the most public presentation of the self of a participant. On the other hand, the roles acting on the most specific context are uni-directional: the most private presentation of the self of a participant. In every context, participants of different roles form various types of relationships among themselves. Each context and all the roles or relationships therein have temporal dimensions. For example, when a student enrolls in a course, their role as a registrant of that course or their relationship with the TA for the evaluation context ends as the course ends. The notion of a relationship is dynamic as it evolves from one interaction to the next.

3 ROLE-BASED AND RELATIONSHIP-BASED IDENTITY MANAGEMENT IN E-LEARNING

In this paper, we employ a purpose-based and recursive notion of context in the e-learning domain (shown in Figure 1). For a well-defined purpose, each participant creates a context by assuming some type of role and negotiating some type of relationship. Each context exists until its underpinning purpose is achieved. Since each role or relationship is contextual, any role or relationship is not valid any longer than that of the relevant context. A context may spawn another more granular context, which in turn may spawn yet another context and so on. A context rewinds all its descendant contexts before it comes to an end. A participant in a context may use either their context-specific temporal (i.e. until the context lives) identity or

more generic identity from any of its progenitor contexts. For example, in a Computer Science course context, a student may use their context-specific role-based identity of type "course registrant", or the student may choose to use more generic role-based identity of type "CMPT-major" from the degree context (i.e. progenitor of the course context).

In building a role and relationship-based identity management system, we have identified the following tasks: identifying relevant roles for different contexts, crafting role-based identities to be used by each participant of a role, allowing each participant to assume multiple roles as they qualify and to switch between roles, facilitating the creation of relationship-based identities for roles to build justifiable relationships, and allowing a guarantor to link historical data to its owner to make them accountable for their actions. As depicted in the Figure 2 and 3 below, a representative system should facilitate the creation of a context for a purpose (e.g. a course context for the offering of a course CMPT111), roles for various job functions in a context (e.g. a registrant role in the context of Course- CMPT111), and relationships for various job functions among roles (e.g. a supervisor-supervisee relationship between an instructor and a marker role).

After authentication, the system generates a context hierarchy for a user, in which each context-node corresponds to the affiliation of the user in a context. Once roles are identified (i.e. a set of tasks expected of a role to perform in a given context is grouped under a role name), a role-based identity creation involves assigning a user to a pertinent role, generating a role-term pseudonym for the user on the assumption of a role, and creating an identity dataset consisting of only role-specific information. Based on their assumed role within a context, the system should allow one user to choose an appropriate relationship with another user, help a user create a relationship-specific identity dataset, and generate a relationship-term pseudonym for the user to be used in a relationship. For providing awareness cues to a user, the system should display the hierarchy of contexts relevant to them together with their assumed roles and relationships therein.

Even though a role-based identity from one context can be used to all the descendant contexts, a relationship-based identity in one context is irrelevant in another context. For example, instead of using her context-specific pseudonym as a registrant of a course, registrant43, a student may choose to appear as cs37, revealing her affiliation to Computer Science department. Other enrollees of that course would not know whether cs37 is a co-registrant in the respective course, an instructor of this course, or a student in the department who may or may not be enrolled in that course. When cs37 seeks technical writing help from the learning centre and creates a relationship-based identity with a writing help, she reveals more personal information. Due to the temporal dimension of role or relationship, any information released under a role or relationship ought to be virtually unusable for the counterpart when the respective role or relationship expires. Anytime, a participant fears a privacy threat in a relationship-based identity, the participant may abandon their respective relationship-based pseudonymous identity and take refuge in their role-based identity. The participant can negotiate a new relationship at any time and craft a new relationship-based identity.

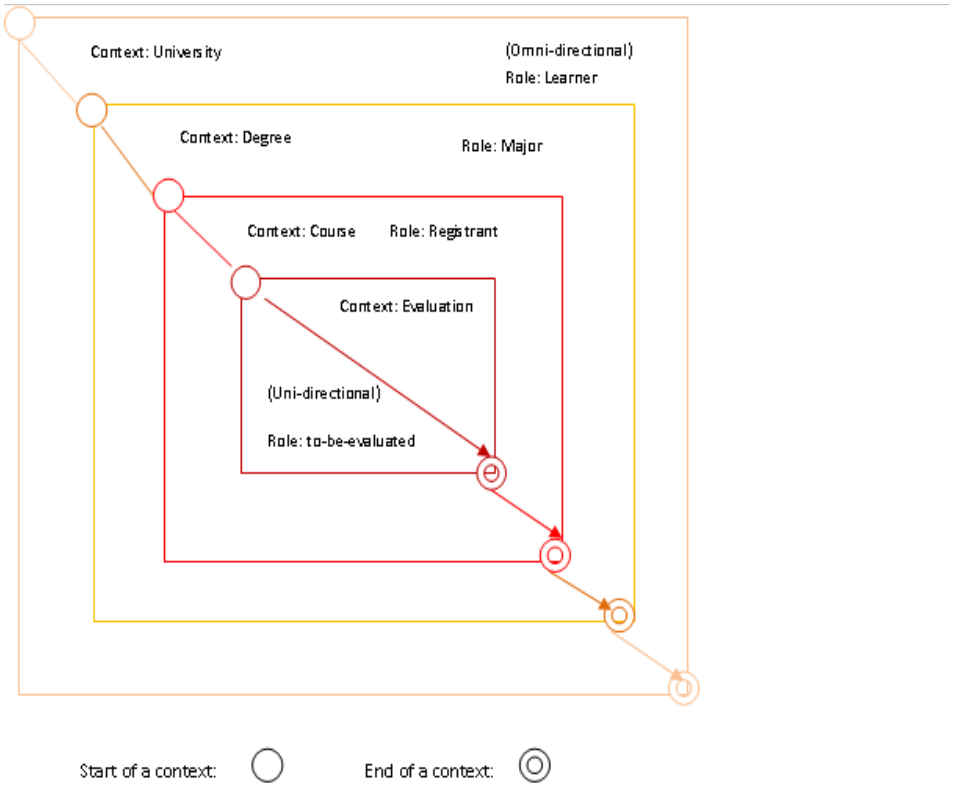

Fig. 1 Contexts of Various Granularities

Ideally, a relationship-based identity is constrained by the purpose of a relationship, which in turn is constrained by the context of the relationship and contextual roles of the participants involved in that relationship. A relationship should not blow the cover of a role, and the identity revealed in a relationship in one context should not be linkable to another context. Since all the participants in the same role carry the same role-based identity, the role-based identity approach provides a degree of anonymity to the participants of a role.

The creation and maintenance of so many role- and relationship- based identities may seem like daunting tasks for users. However, in an e-learning environment, contexts, roles, and relationships are relatively predictable and well-defined. For each user account, the system performs context and role assignments providing a default role-based identity for each role that the user may partake in. The system also enables users to engage in likely relationships (determined by their assumed roles in respective contexts) and provides relationship-based identities. To help users manage their identities, the system provides awareness to users through visualization of contexts, roles, relationships and pseudonyms of them and their partners. Addi-

tionally, the system enforces expiration of context, role, or relationship and tracks information for a cause, which is deemed justifiable by a guarantor.

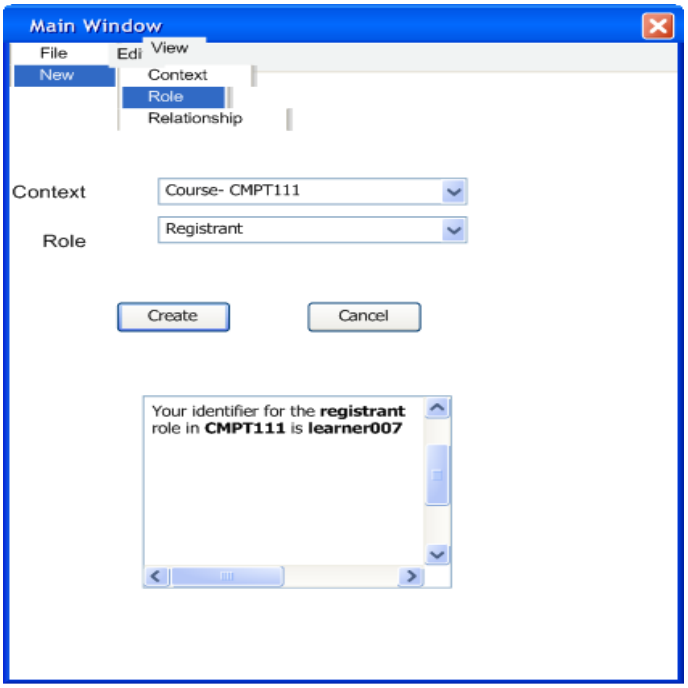

Fig. 2 A Prototype of Role and Relationship Based Identity Management Client

3.1 Example Scenarios

When Alice appears in the freshman orientation of Computer Science Department, her freshman-student role is revealed to the articipants of the program. She may share some comments with the participant sitting next to her. When Alice chooses to befriend that individual, who introduces himself as Bob, she reveals her name to him. Alice and Bob can both uniquely distinguish each other from other freshman Computer Science students. The friendship of Alice and Bob is an example of a relationship. Since one body presents one identity in the physical world, it is hard for Alice to be indistinguishable from other students to Bob. In the disembodied online world, Alice can hide herself in the crowd of fellow students just by choosing her role based pseudonym, A032 (or Abigail or any other unique identifier), and as such have an identity that persists for some time but also remains become indistinguish-

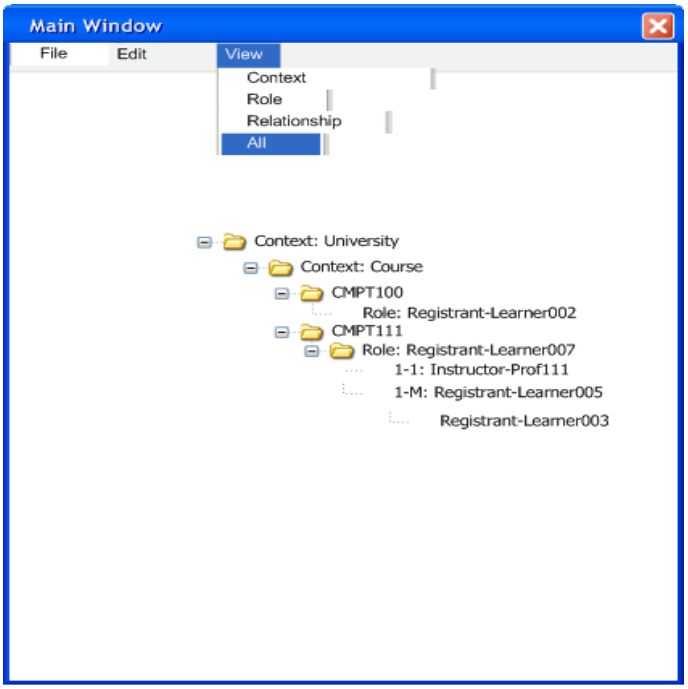

Fig. 3 A Prototype of Role and Relationship Based Identity Management Client

able from other students to Bob. Alice may even renegotiate her relationship with Bob and befriend Bob as A99 (or Antionette).

As shown in Figure 3, a context spawns more granular contexts. For example, Alice wants to go to a college to attain a bachelor's degree. Upon admission, she begins a student context assuming a student role. Her role as a student is the beacon of her identity to the members of the college community. Any member of the college community should at least recognize her as a student of the respective college. As Alice registers in a course for the purpose of fulfilling the course requirements for the degree, she creates another context assuming a role of a registrant (e.g. registrant56). To earn credits from the course, she has to participate in various course-related activities. By participating in each activity, Alice creates even more granular contexts. Each activity may consist of various parts and each part may require building relationships with other actors. Therefore, a context can be presented by an assumed role and relationships built by a participant for a specific purpose. A relationship-based identity (and associated identifier) has to expire by latest the end of the respective role under which the relationship has been initiated. For example, when Alice and Bob want to partner with each other for the group project4 in a course CMPT111, they need to be personable to each other and share each other's schedule, contact information, etc. At the end of the project4, this relationship and the relationship-based identity should expire.

An entity in hierarchical relation may be subjected to prejudice or vindictiveness by the other entities, and therefore, the participants have to be provided with disjoint identities in similar contexts. For example, a 3rd year student Bob bears grudge against a 2nd year student Alice for making derogatory comments about Bob's presentation in the course they took together in the past. As a marker for a course that Alice is currently taking, Bob may act on that grudge against Alice. To prevent this type of situation, Alice's identity from one context (a course) has to be non-linkable to the identity from another related type of context (another course).

3.2 Features of a Role and Relationship Based Identity Management

The privacy solution provided by the proposed role and relationship based identity management is two-fold: on one hand, the role-relationship initiation feature contributes to privacy by constructing contextual identity. On the other hand, forgetting of disclosed information is enforced by the following features: disavowing a relationship, temporal aspect of role and relationship, expiration of context, and disclosure/obligation management. The model also enforces accountability by holding an actor responsible for foul acting through guarantor administered investigation and sanction.

Role-relatonship Initiation: Users are granted membership into roles based on their affiliation to a context in the domain. By taking on an assigned role, an actor assumes an identity warranted by the role. For the purpose of the assumed role, an actor may engage in one of the system-defined relationships and assume an identity warranted by the relationship. By partitioning an identity based on role and relationship, a role/relationship identity management (RRIM) system can provide privacy and restrict information linkage attacks. A role-based identity also provides anonymity for users by making them indistinguishable from other users of the same role.

Disavowing a Relationship: When a relationship is or appears to be privacy threatening for a participant, they can disavow the relationship and disappear in one of their role-based identities. Once returned to a role-based identity, a participant cannot be re-identified to their forgone relationship-based identity. For example, assuming a role-based identity (and corresponding identifier) as a registrant in a course, a learner is known to his fellow learners as a course-mate. Later on, the learner may negotiate a one-to-one relationship with another learner and subsequently choose a relationship-based identity (uni-directional identifier). As time progresses, the relationship may turn out to be disadvantageous for one of the learners and the valuable information released may appear to be at risk. Or, one learner may realize the disclosure of some critical information is extraneous for the respective context. In that situation, the learner could shed their relationship-based identity and put on a role-based identity from the current or any of the ancestor contexts (a registrant of the course or a Computer Science major) and negotiate another rela-

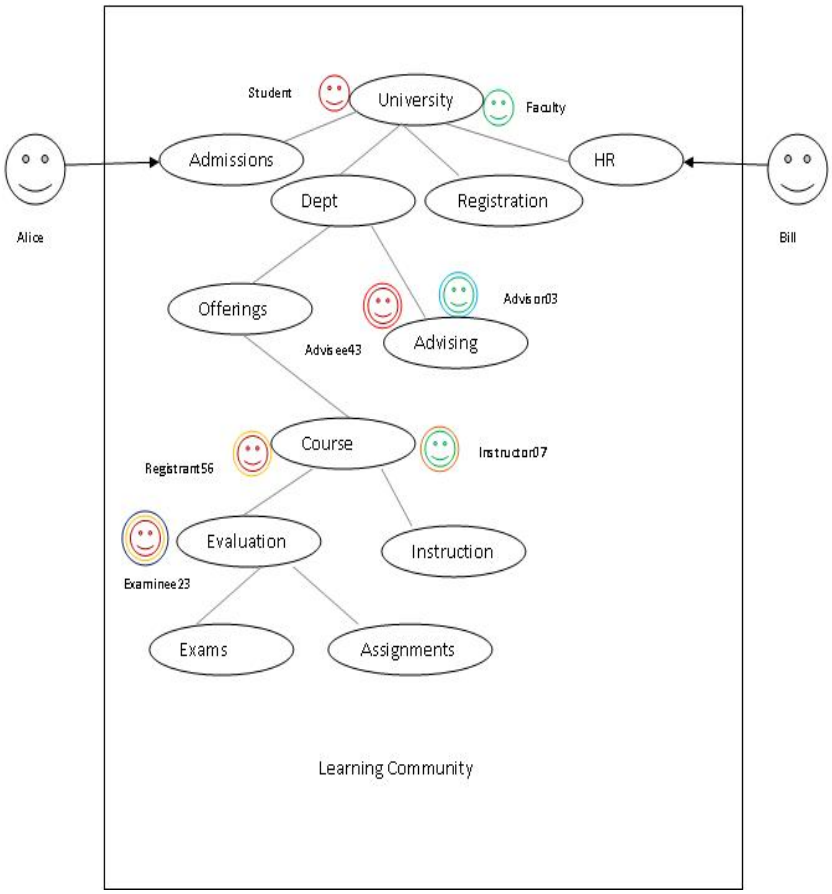

Fig. 4 Role-based Identities of Alice and Bill at Various Contexts

tionship afresh even with the previous partner expiring their previous uni-directional identifier and disassociating disclosed information from their new identity.

Temporal Aspect of Role and Relationship based Identity: Each role and relationship has some type of temporal aspect. After a certain amount of time, a role or a relationship-based identity and corresponding identifier become irrelevant to the context. For example, once a student graduates, their role as a student or their relationship with the housing authority becomes irrelevant. If the above role or relationship-based identity outlives an individual's studentship, it may jeopardize privacy for either that individual or other participants.

Expiration of Context: In an e-learning setting, every context has a purpose. A context may recursively spawn a finer grained context, which contributes to the purpose of their parent context. Once a purpose is achieved, the relevant context winds itself to its parent context. Any information disclosed for the purpose of the defunct context has to be made irrelevant for any other purpose. However, anything

achieved in the defunct context that contributes to its parent context are attached to the participant's assumed role in the parent context.

Disclosure/ Obligation Management: To resolve foul acting, an actor in guarantor role may need to access the disclosed information of a participant. For the sake of transparency, a suspect should be allowed to observe the usage of their disclosed information. An obligation management tool for the guarantor and a disclosure management tool for the participants could help in this regard. Besides, for every possible context, usage guidelines for the disclosed information have to be developed and information receiver should be obligated to follow the guidelines. An information receiver needs to meet various obligations depending on many contexts, and an information giver needs to keep track of information shared with various parties.

Once the underlying purpose is achieved, the respective context or identity is no longer in use leaving no reason for misrepresentation. Once a context ends, information released in that context (under a role or a relationship-based identity) will be archived for a certain amount of time under its parent context for various needs (e.g. user modeling with mutual consent, resolving any complaint, etc.). For any archived information, the information archivist has an obligation regarding information retention or usage. As a context ends, the performance of an identity under that context may be propagated back to its parent context resulting in a backward propagation of values (reputation) from the innermost context to the outermost context. For example, in the outermost context, a person becomes a student for the purpose of attaining a degree. In the innermost context the student is evaluated in an assignment of a course, the student's mark in that assignment is propagated to its parent context of the course and the course grade is eventually propagated backwards to the outermost context contributing to achieving their degree.

Sanction against Foul Acting: Even though participants can disassociate themselves from their role or relationship based identities, they ought to be barred from doing so in case of any questionable action, while an investigation is launched by a participant holding a role with guarantor privileges. The roles perceived as holding the responsibility of a public trustee by other roles (e.g. an instructor in a course) are granted guarantor privilege. As part of a sanction, a participant found guilty of foul acting may be given identity imprisonment. By demonstrating satisfactory conduct, the participant can get digital forgiveness.

Identity Imprisonment: During communication between two actors, as soon as one senses some foul acting by the other, he/she could have the guarantor lock the identifier of the bad actor. In the locking process, complaints against the bad actor are filed to the guarantor of the respective context, and in response, the bad actor's activities are being monitored. Additionally, the bad actor will be restricted to change their existing identifier unless the bad actor is acquitted from complaints, or they have earned good reputation over a period of time. The victim may disown any information disclosed to the bad actor by choosing an omni-directional (indistinguishable) role based identity. Since the victim of the bad acting can identify and reject the bad actor, restricting the change of identifier is a sanction to the bad actor without revealing their true identity. In this way, the penalty for bad action is being condemned to an identity that cannot be shed.

Digital Forgiveness: On the other hand, by self-correcting and displaying good behaviour over a period of time, the bad actor can have the guarantor unlock their identifier with the bad reputation marker and let them choose a new identifier to be free of their haunting past. Once an actor is allowed to disown their guilt-ridden identity, they are forgiven from their committed bad acting. Other participants will no longer be able to identify the participant who has acted foul towards them in the past.

For example, a marker suspects the act of cheating by a student Alice during the marking of assignment1. The marker locks this identifier (i.e. Alice) and thereby reports to the guarantor of this context (i.e. the instructor) about the questionable act. Upon investigation, the instructor may lock the Alice identity for next two assignments that allows the marker to monitor Alice very closely for any further act of cheating. As Alice demonstrates integrity in the next two assignments, the instructor will unlock the Alice identity and allow the participant to assume a new identity. As a result, the participant of Alice identity will not be a victim of prejudice from the marker.

3.3 Worked Examples

In Table 1, we demonstrate the process of role and relationship-based identity management in the iHelp Discussion Forum, which acts as an online forum for students at the University of Saskatchewan to converse asynchronously with one another, with subject matter experts, and with their instructors. For example, as shown in Figure 4, upon logging on to the discussion forum page, a user with the pseudonym learner007 selects CMPT111 context to participate in the CMPT111 forum. As a result, an action menu followed by a list of posting threads for CMPT111 forum shows up on the upper right frame of the page. Then, learner007 may select an appropriate Action from the menu to start a new thread or to reply to an existing thread.

4 RELATED WORKS

In computer science, privacy is addressed from the perspectives of many areas from access control to data integrity to identity management [9]. Goffman's observations set the stage to think about privacy in terms of identity. He states that individuals reveal and conceal information selectively to maintain context-specific identity and social relationship [7]. Demchak and Fenstermacher note that privacy is directly related to the knowledge of identity [6]. A similar notion of privacy is manifested in the work of both Samarati and Sweeney [8, 9]. A general doctrine of their work is to release all the information, but to do so such that the identities of the people who are the subjects of the data (or other sensitive properties found in the data) are

Table 1 Role and Relationship Based Identity Management

Tasks	Processes
Context Constructions	Based on various purposes for discussions, various contexts are enumerated (e.g. University, CMPT, etc.; see oval 1 of Figure 6). Each context is created with a time-to-live time stamp to indicate an end after fulfilling its purpose.
Role-based Identity Constructions	Based on a user's relevance to a context and their expected activities in the context, each user account is granted various potential roles and a default pseudonym (e.g. academic11, learner002, etc.; see oval 2 of Figure 6) per role in various contexts.
Relationship-based Identity Constructions	A user in a given context may requisition for a relationship-based identity for a relationship type permitted for the assumed role (e.g. one-to-one student-teacher relationship) from the system. The system provides a default pseudonym (e.g. Bill; see oval 3 of Figure 6).
Identity Awareness	Each user sees a side-ways contextual identity tree (see Figure 4 & Figure 6) upon logging on to the system. Before submission of a message, a user sees the preview of their message, underpinning context, assumed role, and pseudonym.
Identity Assumptions	Upon a single sign-on, a user may choose a context, role, or relationship node (by left clicking on the node) from the contextual identity tree to participate in a respective capacity under a respective context. A user may right click in a pseudonym of a role in a context and choose from the lists of sub-contexts to use the same identity in the sub-context; see oval 4 of Figure 6).
Identity Expirations	A role- or a relationship- based identity and its associated postings are expunged from the system at the end of its owner context (the context for which the identity is created). If a role-based identity is used at any of the inner contexts of its owner context, the identity and the associated postings are expunged from only that inner context at its end. A user may shed any of their role- or relationship-based identity at anytime unless the identity is locked (see Identity Locking task). For that matter, the user may request the system to remove any message posted under their disowned identity.
Identity Locking	The user of a locked identity is barred from changing their pseudonym, and the user is not allowed to construct a new identity in the same context. For example, when a student with Student11 pseudonym is sanctioned for bad acting in a CMPT250 course forum, that student is locked in their Student11 pseudonym.
Digital Forgiveness	When a bad actor is forgiven, they are allowed to change their pseudonym associated with the foul acting or to create a new identity.When a bad actor is forgiven, they are allowed to change their pseudonym associated with the foul acting or to create a new identity.

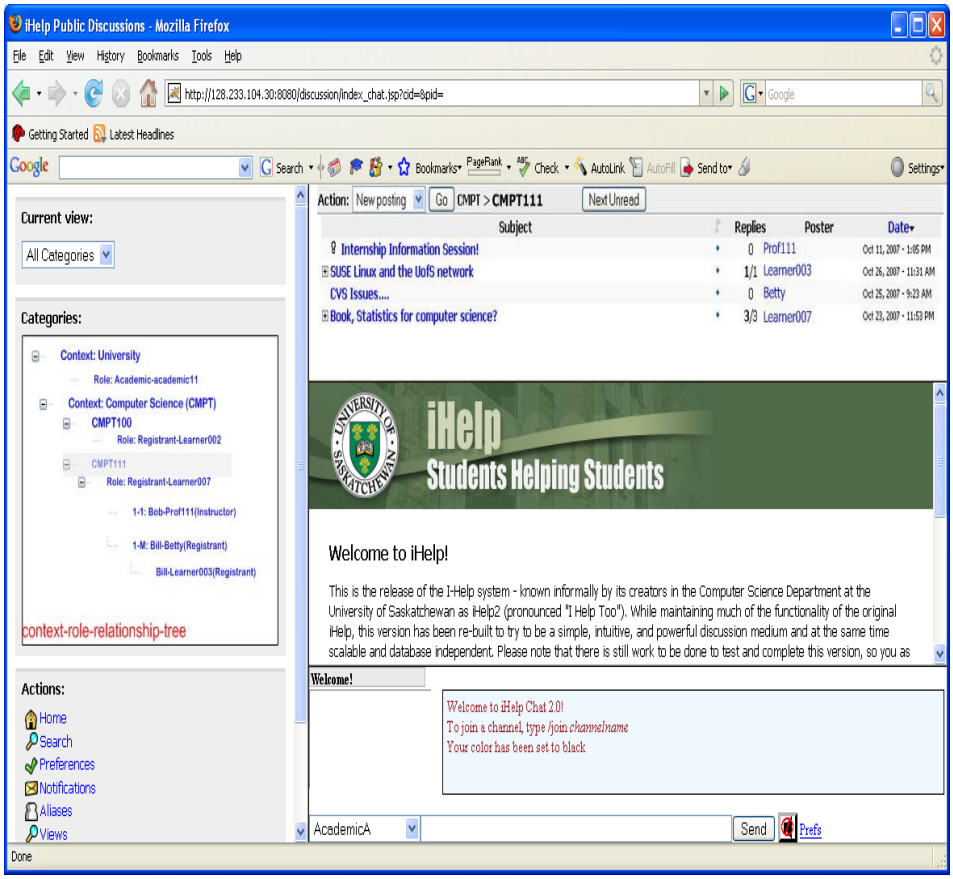

Fig. 5 A Screenshot of iHelp Discussion Forum

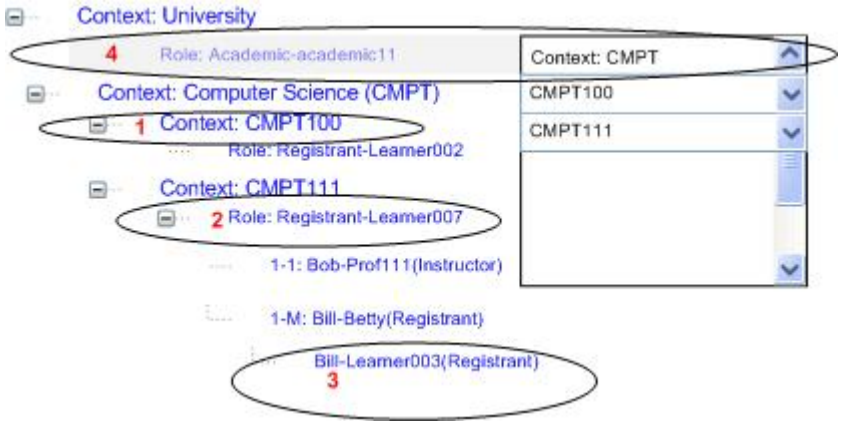

Fig. 6 Explanation of Context-Role-Relationship Tree from Figure 5

protected. In the similar notion, we view that a learner's or a teacher's privacy is their capacity to control the disclosure and usage of their identity information.

Our role- and relationship-based identity approach is inspired by digital identity management approaches appear in the literature [3]. An identity management system helps users to select among the anonymous, pseudonymous, or identified interactions and help them maintain the underlying identity. However, users need to understand context to select and maintain context-specific identities and social relationships. In the real world, our body conveys part of our identities by projecting information about ourselves [5]. In the disembodied online world, we lack adequate contextual cues to understand contexts. Besides, information can proliferate in lighting speed making it hard to understand the true nature of our audience. In the real world, our identity becomes irrelevant or unimportant in most part (except for very few purposes like legacy) with the passing away of our body. However, once an identity is disclosed, it may live in the online space forever. Therefore, an identity management system should facilitate understanding of contexts, crafting of contextual and temporal identities, expiring of identities, and ensuring accountability to help us properly control our identity and thereby preserve privacy.

5 CONCLUSION AND FUTURE WORK

The broad acceptance and adoption of e-learning amplifies the issues of privacy. Unlike the majority of the privacy-related research in the e-learning domain that aims at addressing only learners' privacy, we feel the need for a privacy-enhanced environment to support privacy for all the participants of e-learning. In that vein, we investigated the identity management approach to build a privacy-enhanced e-learning environment. We have identified the following inadequacies of identity management approaches that have appeared in the literature in addressing privacy: a) the notion of context is ambiguous and it is onus of users to understand the context; b) a partial identity of a user does not carry a temporal aspect; c) there is no expiring or reconstructing of a partial identity; and d) balancing of privacy and accountability are not addressed. Focusing on the above mentioned inadequacies, we present a role and relationship-based identity management approach in building a privacy-enhanced e-learning environment.

An important contribution of this work is that it creates a generalizable approach to data expiration. Personal or confidential information that is associated with a pseudonymous individual in a relationship-based identity context becomes disconnected from the person when the context expires. Thus the data itself, even if saved or retained, is disconnected from any individual and thus becomes useless for anyone trying to misuse (or re-use) personal information.

This paper introduces the notion of role- and relationship- based identity management by focusing on the e-learning domain. Since e-learning is an application area that comprises many scenarios, which are common in the digital world, this approach can naturally be adapted into other domains. Once the role hierarchy of a

domain is defined and types of relationships among roles are classified, this model can be applied to that domain to allow participants to construct role and relationship-based identities for purpose-based well-defined contexts. We are in the process of building prototypes of a more general role and relationship-based identity management system. We will verify our prototype with user studies.

References

1. Anwar, M., Greer, J., and Brooks, C.: Privacy Enhanced Personalization in E-learning. In Proceedings of the 2006 International Conference on Privacy, Security, and Trust (PST2006), Markham, Ontario, Canada (2006)
2. Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H.: Towards. Privacy-Aware Elearning. In: G. Danezis, and D. Martin (eds.) Lecture Notes in Computer Science, pp. 167-178. Springer, Heidelberg (2005)
3. Camenisch, J., Shelat, A., Sommer, D., Fischer-Hübner, M. H. S., Krasemann, H., Lacoste, G., Leenes, R., & et al.: Privacy and Identity Management for Everyone. In Proceedings of the workshop on Digital identity management, Fairfax, VA, USA (2005)
4. Cavoukian, A. and Hamilton, T. J.: Privacy Payoff: How Successful Businesses Build Customer Trust. McGraw-Hill Ryerson, (2002)
5. Davis, F.: Fashion, Culture and Identity. University of Chicago Press, Chicago, IL (1992)
6. Demchak, C. C. and Fenstermacher, K. D.: Balancing security and privacy in the information and terrorism age: distinguishing behavior from identity institutionally and technologically. The Forum, 2(2), Article 6, (2004)
7. Goffman, E.: The Presentation of Self in Everyday Life. Doubleday, New York, NY (1959)
8. Samarati, P.: Protecting respondents' identities in microdata release. IEEE Transactions on Knowledge and Data Engineering, 13(6), 1010-1027 (2001)
9. Sweeney, L.: k-Anonymity: A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570 (2002)
10. Westin, A. F.: Privacy and Freedom. Atheneum, New York, NY (1967)