A Semantically-enabled Trust Model for Collaborative Environments

Joaquin Reyna\textsuperscript{1,2}, Natalia Villanueva-Rosas\textsuperscript{1,2,*}, Deana Pennington\textsuperscript{2,4}

\textsuperscript{1}Department of Computer Science, \textsuperscript{2}Cyber-ShARE Center of Excellence, \textsuperscript{3}Department of Geological Sciences, \textsuperscript{*}Faculty Mentor

jareyna2@miners.utep.edu, (n villanuevarosales, dpennington)@utep.edu
The University of Texas at El Paso

Abstract

This poster describes our work towards creating a model of trust in web resources, in particular academic resources. This model is inspired by Google’s famous algorithm PageRank and takes into account users, credentials for said users, resources and tags pertaining to both; it deals with the exchange and propagation of trust. The system was implemented in the Virtual Learning Commons collaborative environment, developed and hosted by the Cyber-ShARE Center of Excellence at the University of Texas at El Paso.

Introduction

The automated creation and management of trust is a challenge in web environments where anyone can upload resources and their reliability is in question. Finding trustworthy information is key in academia where information is used to advance the state of the art.

Background

Research for creating and managing trust can be categorized as [2]:

1. Policy-based trust – Focusing on exchanging credentials and enforcing access policies.
2. Reputation-based trust - Using past interactions of an entity to assess its future behavior.
3. General models of trust - Modeling trust in different domains.
4. Trust in information resources - Capturing ratings from users about the quality of resources, propagating trust over links, among others.

Our work falls between the categories of reputation-based trust and trust in information resources. Related work typically focuses on e-commerce while our solution focuses on an academic setting.

Algorithm

Key features of the proposed algorithm:

1. Use of domain of knowledge. Users and resources are assigned trust based on user credentials and interactions tied to specific subject fields (e.g., a user’s knowledge in the fields of Geology and Computer Science may differ).
2. Use of user credentials and interactions. The trust assigned to users (Fig. 2) is the aggregation of two values (credentials + interactions). For the credentials part of the calculation we multiply a value representing their academic level times the average endorsement value on the system. The second value is the aggregation of the trust of the resources they have uploaded.
3. Use of endorsements. The trust assigned to resources comes from user endorsements (Fig. 3). When a user makes an endorsement, user’s trust is divided evenly among all his/her endorsements. The change in trust is then propagated to all connected nodes in the system.

Function getTrust(user)

\begin{verbatim}
trust = getTrust(user);
if upload in user uploads:
    trust = upload trust;
return trust;
\end{verbatim}

Fig. 2. Algorithm pseudo-code to calculate user trust.

Future Work

The next step is to validate the system using VLC users’ input. The algorithm can be improved in a couple of ways, namely some variations of the algorithms are worthy of study. One such variation would give users with high credentials a field higher trust in related subjects (e.g., Microbiology and Macrobiology).

References