A Dynamic Trust Estimation Method for 'Persona' from the Human Relationship of Social Web

Social Web and Trust by the Rating of a Persona's Active Audience

Shigeichiro YAMASAKI/ Kinki University
Faculty of Humanity-Oriented Science and Engineering
Department of Information and Computer Sciences
Fukuoka, Japan
E-mail: Yamasaki@fuk.kindai.ac.jp

***Abstract*—In this paper, we propose a trust estimation method for a parson by the rating of his or her active audience of social web such as Twitter. We call this method 'trust by the rating of a persona's active audience.' A 'persona', such as 'Display Name' of Twitter (with additional authentication) or 'Claimed ID' of OpenID, denotes an artificial identity to represent one's social position in the user-centric authorization. We utilize the 'persona' to be an object to accumulate the rating of trust for IT services for our trust estimation method. The most significant difference of our trust model and traditional one like PKI is that the trustworthiness of persona is not stable. Therefore, we focused on the implement methods for the sensitivity of the temporal change of a persona's trustworthiness. The basic idea of our 'trust by the rating of a persona's active audience' is similar to the Google Page Rank method. We also try to show that this kind of social web based trust has a possibility to be a global infrastructure for trust.**

Keywords-component; Trust estimation, OAuth, OpenID, Twitter, Trust, Persona; Social Web, Google Page Rank, Privacy, User centric Authorization, Personalized mashup;

I. INTRODUCTION

In the past years, there had been made various efforts to construct the trust and the authentication infrastructure for IT services. PKI and SAML are the examples of them. However, such efforts have not been succeeded until now. While the unpopularity of PKI or SAML, the user-centric authentication systems like OpenID become popular. The purpose of this paper is to propose a method to construct a global-scale trust infrastructure for IT services from the user-centric authorization and the social web service.

A. User-centric authorization and 'persona'

User-centric authentications and authorizations such as OpenID or OAuth are made use of cross-website safe mash-up for personal data exchange. In user-centric authorization, a 'persona', such as 'Display Name' of Twitter or 'Claimed ID' of OpenID, denotes an artificial identity to represent one's social position.

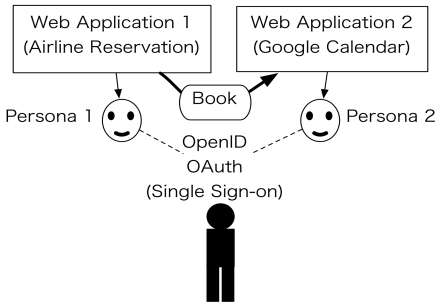

Figure 1. Cross web site safe mash-up for personal data exchange

B. Persona and Privacy

The 'persona' is useful for protecting and controlling personal information and behavior. Some kinds of persona may use for exposure of illegal act. Such kind of persona will be created and destroyed temporally by its owner person. We also may use personas to switch private or public human communication.

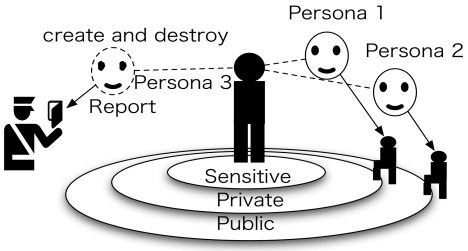

Figure 2. Persona and privacy

C. Accumulation of rating of the persona

A persona also be an object for accumulating one's positive rating. Notice that because every one who own the persona may destroy and re-create it freely, the negative rating of persona will not work well. However, there is an incentive to keep a persona who has positive rating to accumulate the rating.

978-0-7695-4107-5/10 $26.00 © 2010 IEEE
DOI 10.1109/SAINT.2010.51

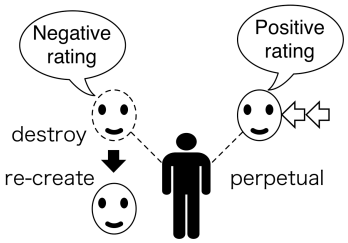

Figure 3. Negative rating and positive rating of persona

D. Social Web as an ecosystem for trust infrastructure

The standing point of the trust model of PKI and SAML is the trustable authority. Beside this, the standing point of the trust model of social web is the results of the activities of a person and estimation from the other people for them. The trust by authority is static and the trust by social web is dynamic. We should treat the social web based dynamic trust infrastructure to be a kind of eco-system.

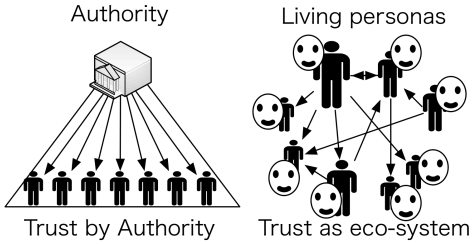

Figure 4. Static model and dynamic model for trust infrastructure

E. Global-scale trust infrastructure by the user-centric authorization

Global scale mutual authentication and authorization tend to cause various complicated problems. For example, international PKI or SAML based authorization has succeeded only few limited area.

One of the purposes of our research is to construct the practical and lightweight inter-national mutual trust infrastructure without complicated governmental control.

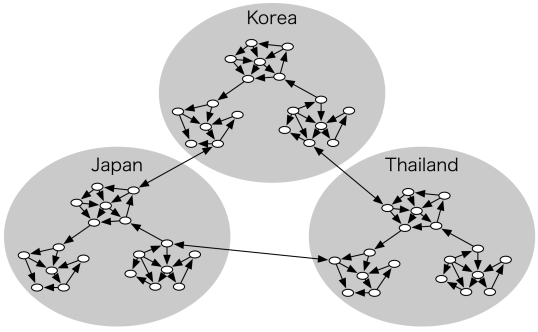

Figure 5. Inter national mutual trust infrastructure

II. TRUST BY THE RATING OF ONE'S ACTIVE AUDIENCE

We propose a trust model that is based on the notion of 'active audience' of the Social Web and its estimation methods.

The basic idea of our proposal about the rating for trust is similar to the Google's Page Rank method. Google Page Rank is an evaluation method for the importance of a web page from the results of searching.

A. Recommendation of a persona's statements

The features of Google Page Rank are (1) a hyperlink of a web page considered to be a recommendation of it, (2) a web page that is referred from many web pages will be an important page, (3) a page which is referred from the important page also will be an important page.

We chose Twitter as a good example of Social Web. We try to propose that active audience relation among Twitter is able to regarded to be a hyperlink.

The basic relationship of Twitter is to follow a persona from another persona. We consider this follower-followed relationship among personas to be a recommendation of the followed persona's statements from the follower. A 'Time line' of Twitter means the temporally sequenced messages of followed personas. The real object of the recommendation is the 'time line' of the followed persona. The intuitive meaning of 'the rank of a persona' is the average of the recommendation rate of the persona.

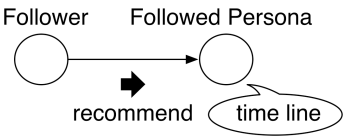

Figure 6. Follower followed relation of Twitter as recommendation

B. Authority type persona and distibuter type persona

In our trust model a persona who has many follower is defined as an authority type persona.

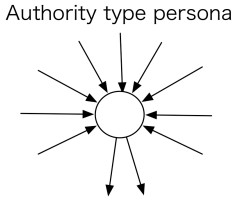

Figure 7. Authority type persona

C. Rating of the followed persona of an authority type persona

A followed persona who is followed by an authority type persona may also be an authority type. Although its authority rating is dependent on the number of out links (following) of the follower authority. If the follower authority follows only few personas, the followed one's rating should be high. If the authority has many followers, the followed one's rating will be lower than the former case.

Notice that, in our trust model a rating of trust is not decided by the following relationship but the 'active audience' relationship. The numbers of follower and followed personas are useful information for approximation to calculate our trust rating.

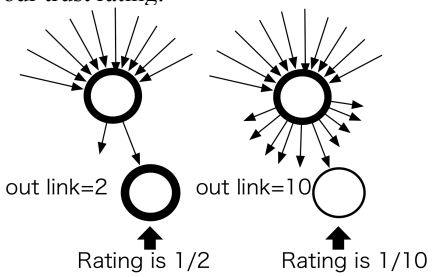

Figure 8. The rating of the followed persona of an authority

D. Active Audience as actual number of out link

The active audiences are the personas who actually get the message from their following persona. If a persona is not logged in the Twitter system then the persona is not the active audience currently.

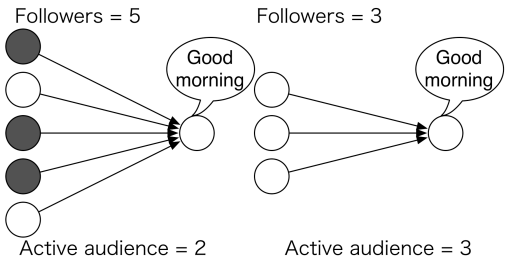

Figure 9. The number of active audience of followers

E. 'Temporal Similarity' of Active Audience

The estimation method of active audience is required time scales. The most important time scale is one day because active audiences will share the temporal lifestyle in typical one day with the followed persona.

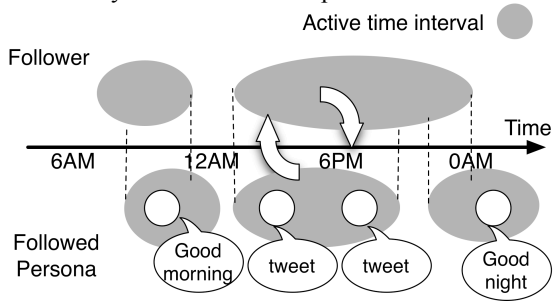

Figure 10. Two personas who share the temporal lifestyle

Temporal similarity of a persona and a follower is defined by the ratio of overlapped active time intervals of a persona and the follower in one day.

F. Re-tweeting and active audience

In Twitter, one's utterance can be forwarded by his or her followers. It called 'Re-tweeting.' Re-tweeting is very important factor to estimate the rating of the original speaker because it is an evidence of the utterance is valuable for the followers of some follower. Re-tweeted message might be Re-tweeted by the follower's follower.

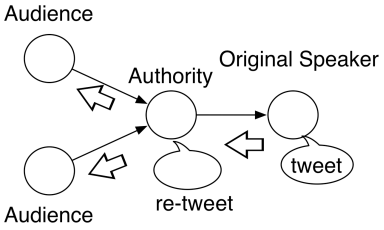

Figure 11. Re-tweeting and the message distribution

G. Goolge Page Rank

The basic idea of Google Page Rank method is as below. This method is very simple and elegant. Some efficient calculation method to get Google matrix G is known.

$r(P_i)$: The rank of P_i
B_{P_i} : Back link pages of P_i
$|P_i|$: The out degree of P_i

$$r(P_i) = \sum_{P_j \in B_{P_i}} \frac{r(P_j)}{|P_j|} \quad (1)$$

$$\mathbf{H}_{ij} = \frac{1}{|P_i|}$$

$\mathbf{H}$: Sub-stochastic hyper-link matrix
$\mathbf{a}$: Dangling node vector
α : Scaling parameter
$\mathbf{e}$: Row vector (every element is 1).

$$\mathbf{G} = \alpha\mathbf{H} + (\alpha\mathbf{a} + (1-\alpha)\mathbf{e})\frac{1}{n\mathbf{e}^T} \quad (2)$$

H. Our Model correspond to the Google Page Rank

A 'Page' correspond to a 'persona.'

The 'Rank of a Page' correspond to the 'Rank of a persona.'

'Back link pages of a page' correspond to the 'time lines of active audiences of a persona' and the 'active audience' means the average of the temporal simirality of the persona's follower and a follower of active followers if some utterance had been Re-tweeted by the follower.

The 'out degree of a page' correspond to the 'number of the following personas.'

The 'dangling node' means a node which has no out link. In our model the dangling node correspond to a persona who does not follow any other persona. The element of the dangling node vector is a probability of to move any persona all over the world by key word searching.

The scaling parameter is a parameter for adjustment.

III. PROBLEMS TO SOLVE AND OUR APPROACH

A. *Sensitivity of the change of trustworthiness of a persona*

The first problem is that how we can quickly sense the decline or the increase the persona's rating of trust over the huge scale human relationship of Social Web.

B. *How to sense the change of trustworthiness of a persona quickly*

Clustering the human relationship over the Social Web and restrict the range of re-calculation of trust rating to the cluster.

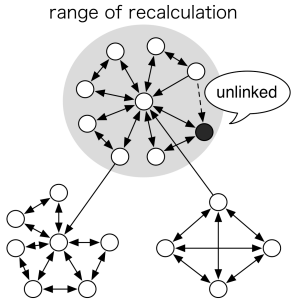

Figure 12. Cluster and range of re-calculation

The personas of a cluster have some common fratures and such kind of similarity is an important factor of trust because people tend to trust a person who resembles him or her. The range of re-calculation can be restricted the cluster which has the most similarity to the subjective persona.

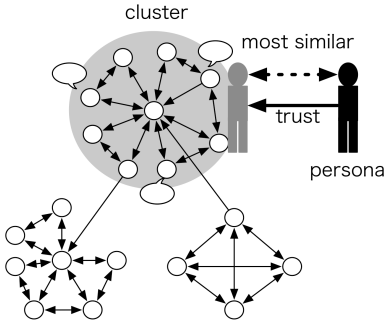

Figure 13. Similarity of persona and range of re-calculation.

Moreover, we can restrict the range of re-calculation of trust rating by the common language.

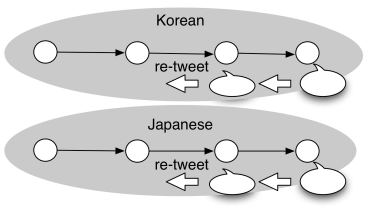

Figure 14. Clustering by language

C. *How to distinguish software robot from human persona*

To prove the actual existence of a persona is a basic and important requirement of trust infrastructure. However, essentially no one can distinguish a clever software robot from the human persona in Twitter.

To avoid this problem, the user authentication infrastructure with the identity confirmation policy exchange like a PAPE (Provider Authentication Policy Extension) of OpenID is important. The reliability or trustworthiness of OpenID provider is another problem to solve.

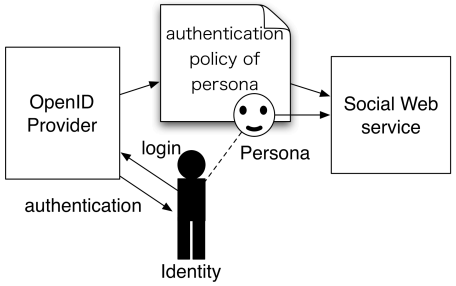

Figure 15. How to distinguish a bot from an actual human

IV. CONCLUSION AND FUTURE WORK

In this paper we have propose an estimation method for a persona from the human relationship of social web services such as Twitter.

Our implementation is only small size now. We should examine the large scaled system and should evaluate the efficiency and usability of our proposal.

The current specification of Twitter is not sufficient for our trust infrastructure. We hope our research contributes to a sound evolution of Social Web.

[1] Alexandre Passant, et al.; Enabling Trust and Privacy on the Social Web, W3C Workshop on the Future of Social Networking, 15-16 January 2009

[2] OASIS.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[3] Mark Atwood, et al.: OAuth Core 1.0, http://oauth.net/, 2007

[4] OpenID Community: OpenID Authentication 2.0 Final, http://openid.net/specs/openid-authentication2-0.html, 2007

[5] D. Recordon et al.: OpenID Provider Authentication Policy Extension 1.0, http://openid.net/specs/openid-provider-authentication-policy-extension-10.html

[6] Amy N. Langville and Carl D. Meyer, "GOOGLE'S PAGE RANK AND BEYOND," Prinston University Press