Volume 2, Issue 11, November-2015, pp. 727-732 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

A Computational Dynamic Trust Model for User Authorization

[1]K.S. Harika Hampi, [2]Prof. C.Uma Shankar , [3]Dr. S.Prem Kumar

[1]Pursuing M.Tech, CSE Branch,Dept of CSE
[2]Registar Rastriya Sanskrit Vidyapeetha Tirupathi.Andhra Pradesh,India.
[3]Professor & HOD, Department of computer science and engineering,
[1,2]G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract:- Improvement of authorization process for protected information access by a large society of users in an open environment is an important problem in today's Internet world. In this paper we propose a computational dynamic trust model for user authorization, rooted in findings from social science. Unlike most existing computational trust models, this model distinguishes trusting belief in integrity from that in capability in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different trusters. Many Model studies were conducted to evaluate the presentation of the proposed integrity belief model with other trust models from the creative writing for different user behavior patterns. Results showed that the proposed model resulted in higher performance than other models especially in predicting the behavior of unbalanced users.

Key Words- Authorization, security, trust, social-science

1. INTRODUCTION

Growing wealth of information available in online have made more secure by obtaining mechanisms on systems today's world. The user authorization mechanisms in today's environment are mostly centre on role-based access control (RBAC). It is a mechanism where it divides the authorization process in to the role-permission and user-role assignment. RBAC in modern systems uses digital identity as facts about a user to allow access to resources which the user is allowed. On the other hand, holding evidence does not necessarily certify a user's good behavior. For example, when a bank is deciding whether to issue a loan to a customer, it does not only required proof such as social security number and home address, but also checks the belief about the applicant, formed based on previous behavior. Such belief, which we call dynamic trusting belief, can be used to calculate the possibility that a user will not perform risky actions. In this effort, we propose a computational dynamic trust model for user authorization. Mechanisms for building trusting belief by means of the direct experience which we can also call first-hand information as well as recommendation and reputation process which is also called as second-hand information are integrated in this model. The hand-outs of the model are:

- The model is embedded in findings from social science i.e. it provides automated trust management that mimics trusting behaviors in the public, bringing trust computation for the society closer to estimate of trust in the real world.
- Dissimilar to other trust models, the proposed model will have records for different types of trust. Particularly, this model distinguishes trusting belief in integrity from other models
- The proposed model takes into consideration about the prejudice of trust ratings by different entities, and set up a mechanism to take away the impact of subjectivity in reputation aggregation. Observed evaluation supports that the difference between competence and integrity trust is necessary

in decision-making. Distinguishing between integrity and competence permits the model to make more informed and fine-grained authorization decisions in different circumstances. Let us consider some examples:

1. Consider an example of real estate consultancy site, competence consists of elements such as finding the best plot area, the best construction, the Interior facilities etc., where as integrity trust is based on factors like whether the site puts fraudulent charges on the customer. In a context where better deals are valued higher than the potential fraud risks, an agency with lower integrity trust could be preferred due to higher competence.

2. Consider an online site which is providing seasonal offers for customers to attract, the capability trust of a seller can be determined by how fast the seller ships the product or product quality etc., each being a different competence type. The integrity trust can be determined by whether he/she sells buyers' information to other parties without buyer permission. In the case of an urgent purchase, a seller with low integrity trust can be allowed if he/she has high competence trust.

3. In support of a web service, the competence trust can include factors such as response time, quality of results etc., whereas integrity trust can depend on whether the service outsources requests to untrusted parties. Tentative evaluation of the proposed integrity belief model in a simulated environment of entities with different behavior patterns propose that the model is able to give better estimations of integrity trust behavior than other major trust computation models, especially in the case of trustees with changing behavior.

2. LITERATURE REVIEW:

2.1 McKnight's Trust Model, The social trust model, which guide the design of the computational model in this paper, was proposed by McKnight et al. [16] after analyzing many papers across a wide range of disciplines. It has been validated via empirical study [15]. This model describes five conceptual trust types: trusting behavior, trusting intention, trusting belief, institution-based trust, and disposition to trust. Trusting behavior is an action that increases a truster's risk or makes the truster to expose to the trustee. Trusting intention specifies that a truster is willing to connect in trusting behaviors with the trustee. A trusting intention involves a trust decision and leads to a trusting behavior. Trusting belief is a truster's subjective faith in the fact that a trustee has attributes beneficial to the truster. Two subtypes of institution-based trust are:

1. Structural pledge: The faith that structures organize promote positive outcomes. Structures include guarantees, policies, assurance etc.

2. Situational normality: The belief that the properly ordered environments facilitate success outcomes. Disposition to trust characterizes a thruster's general propensity to depend on others across a broad spectrum of situations. Institution-based trust depends on situation. Disposition to trust is independent of situation and trustee. Trusting belief positively relates to trusting intention, which in turn results in the trusting behavior. Institution-based trust positively influence on trusting belief and trusting intention. Structural pledge is more related to trusting intention while situational normality affects both. Disposition to trust positively manipulate institution-based trust, trusting belief and trusting intention. Confidence in humanity impact trusting belief. Trusting stance influences trusting intention.

2.2 Computational Trust Models, The problem of launching and maintaining dynamic trust has fascinated much research hard work. One of the first efforts trying to celebrate trust in computer science was made by Marsh [13]. The model introduced the concepts extensively used by other researchers such as context and situational trust. Many existing reputation models and security mechanisms rely on a social network structure [1]. Pujol et al. propose an approach to mine reputation from the social network topology that encodes reputation information [19]. Lang [9] proposes a trust model for access control in P2P networks, based on the assumption of transitivity of trust in social networks, where a simple mathematical model based on fuzzy set membership is used to calculate the trustworthiness of each node in a trust graph symbolizing interactions between network nodes. FCTrust [8] utilises the transaction density

and similarity to calculate a measure of reliability of each recommender in a P2P network. Its main disadvantages are that it has to regain all transactions within a certain time period to estimate trust, which imposes a big performance penalty, and that it does not distinguish between recent and old transactions. Matt et al. [14] introduced a method for modeling the trust of a given agent in a multiagent system by joining statistical information regarding the past behavior of the agent with the agent's usual upcoming behavior. Zhu et al. [26] introduces a dynamic role based access control model for grid computing. The model determines authorization for a specific user based on its role, task and the context, where the authorization decision is updated dynamically by a monitoring module keeping track of user attributes, service attributes and the environment. Fan et al. [5] proposed a similar trust model for grid computing, which focuses on the dynamic change of roles of services. Nagarajan et al. [18] propose a security model for trusted platform based services based on evaluation of past evidence with an exponential time decay function. The model evaluates trust separately for each property of each component of a platform, similar to the consideration of competence trust in our proposed model. Although these approaches integrate context into trust computation, their application is limited to specific domains different from the one considered in our work. Walter et al. [22] proposed a dynamic trust model for social networks, based on the concept of feedback centrality. The model, which enables computing trust between two disconnected nodes in the network through their neighbor nodes, is suitable for application to recommender systems.

3. SYSTEM STUDY

Existing System:

The everyday increasing wealth of information available online has made secure information access mechanisms an indispensable part of information systems today. The mainstream research efforts for user authorization mechanisms in environments where a potential user's permission set is not predefined mostly focus on role-based access control (RBAC), which divides the authorization process into the role-permission and user-role assignment. RBAC in modern systems uses digital identity as evidence about a user to grant access to resources the user is entitled to.

Disadvantages: Holding evidence does not necessarily certify a user's good behavior.

Proposed System:

We propose a computational dynamic trust model for user authorization. Mechanisms for building trusting belief using the first-hand (direct experience) as well as second-hand information (recommendation and reputation) are integrated into the model. The contributions
of the model to computational trust literature are:

- The model is rooted in findings from social science, i.e. it provides automated trust management that mimics trusting behaviors in the society, bringing trust computation

For the digital world closer to the evaluation of trust in the real world.

- Unlike other trust models in the literature, the proposed model accounts for different types of trust. Specifically, it distinguishes trusting belief in integrity from that in competence.
- The model takes into account the subjectivity of trust ratings by different entities, and introduces a mechanism to eliminate the impact of subjectivity in reputation aggregation.

4. SUMMARY OF THE TRUST MODEL:

The trust models we propose in this paper differentiate integrity trust from competence trust. Competence trust is the trusting belief in a trustee's capability or proficiency to perform certain tasks in a exact state. Integrity trust is the belief that a trustee is truthful and acts in support of the truster. Integrity and kindness in social trust models are combined together.

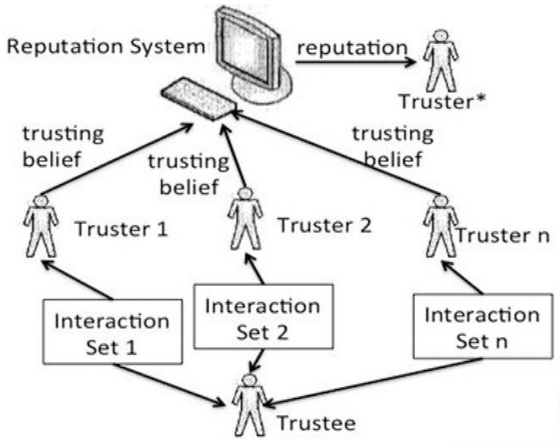

Fig. 1. Model elements

The elements of the model environment, as seen in Fig. 1, include two main types of actors, namely trusters and trustees, a record of trust information, and different framework, which depend on the concerns of a truster and the capability of a trustee.

4.1 Context and Trusting Belief Context: Both trusters concern and trustees behavior vary from one state to another state. These situations are called contexts. A truster can denote the minimum trusting belief needed for a specific context. Direct experience information is maintained for each individual context to speed up belief updating. In this model, a truster has one reliability trust per trustee in all contexts. If a trustee dissatisfies a truster, the misbehavior lowers the truster's integrity belief in him. For integrity trust, contexts do not need to be illustrious. Competence trust is context-dependent.

4.2 Operations Defined on Trust Model :

This segment presents the operations defined on the trust model.

4.2.1 Building and testing trusting beliefs Different techniques are used under various conditions for building and testing trusting beliefs. A candidate method set includes the methods considered in a specific situation. A method is appropriate only if:

(1) It is in the current candidate method set, and (2) its precondition holds.

Building and testing initial competence trust: There are four scenarios when t1 is about to establish initial trust about u1 in c: (1) both c and u1 are new; (2) c is recognized but u1 is new; (3) c is new but u1 is recognized; (4) both c and u1 are recognized. A context c is known if the truster has experience with some trustee in c. A trustee u1 is recognized if she interacted with t1 before. The candidate method set for all scenarios and the order of their priorities are summarized in Table 1. > is a partial order defined on the method priority set. The relationship between two methods enclosed in one "{}" is undefined by the model itself. This is an ambiguous priority set is extended to a total order according to t1's method preference policies.

TABLE 1
CANDIDATE METHOD SET TO BUILD INITIAL COMPETENCE TRUST

	c is new	c is recognized
u1 is new	{M4}≻ {M6, M7}	{M4 }≻ {M5, M7}
u1 is recognized	{M2, M3, M4}≻ {M7}	{M2, M3, M4} ≻ {M5, M7}

The algorithm to build and test an initial competence trusting belief is shown in Fig. 2. The algorithm initializes unused MS using the appropriate candidate method set. It chooses the applicable method M with highest priority in unused. The input threshold parameters δc and δp are compared with the trusting belief generated by M. If "true'" or "false" is obtained, this result is output. Otherwise M is removed, trusting belief is saved and the process is repeated with the next M. In the case that the algorithm outputs no result after all methods do considered, one trust
belief is chosen (i.e. r is chosen among all results) based on imprecision handling policies. The value of the belief is compared with δc.

Fig 2. Algorithm to build/test initial competence trusting belief.

```
Input: t1, u1, c, δc, δp
Output : true/false
 unusedMS := candidate method set defined in
Table 1
i := 1
while unusedMS ≠ Ø {
M := the applicable method with highest priority
result[i] := compute(TC^v_t1→u1(c), TC^p_t1→u1(c)) using
M
testResult := compare result[i] with δc ,δp based
on Table 1
 if (testResult = uncertain)
{
i := i + 1; delete M from unusedMS
}
Else
{
return testResult
}
 }
Choose r from {results[i]U0} based on imprecision
handling policy
return (r.value > δc)
```

4.2. Belief information and reputation Aggregation methods:

Belief about a trustee's competence is context specific. A trustee's competence changes relatively slowly with time. Therefore, competence ratings assigned to her are viewed as samples drawn from a distribution with a steady mean and variance. Competence belief formation is formulated as a parameter estimation problem. Statistic methods are applied on the rating sequence to estimate the steady mean and variance, which are used as the belief value about the trustee's competence and the associated predictability.

5. CONCLUSION

In this paper we presented a dynamic computational trust model for user authorization. This model is ingrained in answering from social science, and is not restricted to trusting belief as most computational methods are. We presented a demonstration of context and functions that relate dissimilar contexts, enabling Building and testing initial competence trust. The proposed dynamic trust model enables automated trust management that mimics trusting behaviors in the public, such as selecting a community partner, forming a association, or choosing conciliation protocols in e-commerce. The formalization of trust helps in scheming algorithms to choose dependable resources in peer-to-peer systems, budding secure protocols for ad hoc networks and detecting unreliable agents in a virtual community. Experiments in a virtual trust environment show that the proposed integrity trust model carrys out better than other major trust models in calculating the behavior of users whose behaviour transform based on certain patterns over time.

6. FUTURE ENHANCEMENT:

The Future enhancement for this paper will be not only allocating dynamic computational trust model for user authorization but also distributing a Dynamic Trust Computation Model for safe Communication in Multi-Agent Systems.

REFERENCES

[1] G.R. Barnes and P.B. Cerrito, "A mathematical model for interpersonal relationships in social networks," Social Networks, vol. 20, no. 2, pp. 179-196, 1998.

[2] R. Brent, Algorithms for Minimization Without Derivatives. Englewood Cliffs, NJ: Prentice-Hall, 1973.

[3] A. Das, and M.M. Islam. "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems," IEEE Trans. Dependable Sec. Comput., vol. 9, no. 2, pp. 261-274, 2012.

[4] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in Proc. 2nd ACM Conference on Electronic Commerce, 2000, pp. 150-157.

[5] L. Fan et al., "A grid authorization mechanism with dynamic role based on trust model," Journal of Computational Information Systems, vol. 8, no. 12, pp. 5077-5084, 2012.
[6] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Communications Surveys, vol. 3, no. 4, pp. 2-16, 2000.
[7] J.D. Hamilton, Time Series Analysis. Princeton, NJ: Princeton University Press, 1994.
[8] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," In Proc. IEEE Ninth Int'l Conf. Young Computer Scientists (ICYCS '08), 2008, pp. 1963-1968.
[9] B. Lang, "A Computational Trust Model for Access Control in P2P," Science China Information Sciences, vol. 53, no. 5, pp. 896-910, May, 2010.
[10] C. Liu and L. Liu, "A trust evaluation model for dynamic authorization," In Proc. International Conference on Computational Intelligence and Software Engineering (CiSE), 2010, pp. 1-4.
[11] X. Long, and J. Joshi, "BaRMS: A Bayesian Reputation Management Approach for P2P Systems," Journal of Information & Knowledge Management, vol. 10, no. 3, pp. 341-349, 2011.
12] S. Ma and J. He, "A Multi-dimension dynamic trust evaluation model based on GA," In Proc. 2nd International Workshop on Intelligent Systems and Applications, 2010, pp. 1-4.
[13] S. Marsh, "Formalizing Trust as a Concept," Ph.D. dissertation, Dept . Comp. Science and Math., Univ. Stirling, U.K., 1994.
[14] P. Matt, M. Morge and F. Toni, "Combining Statistics and Arguments to Compute Trust," In Proc. AAMAS, 2010, pp. 209-216.
[15] D. McKnight, V. Choudhury and C. Kacmar, "Developing and validating trust measures for e-commerce: an integrative topology," Information Systems Research, vol. 13, no. 3, pp. 334-359, September, 2002.
[16] D. McKnight and N.L. Chervany, "Conceptualizing trust: a typology and e-commerce customer relationship model," In Proc. HICSS-34, 2001.
[17] W. Mendenhall and R.J. Beaver, Introduction to Probability and Statistics. Boston, MA: PWS-Kent Pub. Co., 1991.
[18] A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," Future Generation Computer Systems, vol. 27, pp. 564-573, 2011.
[19] J.M. Pujol, R. Sangesa and J. Delgado, "Extracting reputation in multi agent systems by means of social network topology," In Proc. AAMAS, 2002, pp. 467-474.
[20] J. Sabater and C. Sierra, "Social ReGreT, a reputation model based on social relations," ACM SIGecom Exchanges, vol. 3, no. 1, pp. 44-56, 2002.
[21] F. Skopik, D. Schall and S. Dustdar, "Modeling and mining of dynamic trust in complex service-oriented systems," Information Systems, vol. 35, pp. 735-757, 2010.
[22] F.E. Walter, S. Battiston and F. Schweitzer, "Personalized and Dynamic Trust in Social Networks," In Proc. ACM Conference on Recommender Systems (RecSys'09), 2009, pp. 197-204.
[23] X. Wang and L. Wang, "P2P Recommendation Trust Model," In Proc. IEEE Eighth Int'l Conf. Intelligent Systems Design and Applications (ISDA '08), 2008, pp. 591-595.
[24] B. Yu and M.P. Singh, "An evidential model of distributed reputation management," In Proc. AAMAS, 2002, pp. 294-301.
[25] Y. Zhang, S. Chen and G. Yang, "SFTrust: A Double Trust Metric Based Trust Model in Unstructured P2P Systems," In Proc. IEEE Int'l Symp. Parallel and Distributed Processing (ISPDP '09), 2009, pp. 1-7.

