USER AUTHORIZATION WITH AN IMPROVED COMPUTATIONAL DYNAMIC TRUST MODEL

1.T. VINEETHA
UG Scholar,
Department of CSE,
CMR Technical Campus, Hyderabad

2.**REGONDA. NAGARAJU**
Associate Professor,
Department of CSE,
CMR Technical Campus,
Hyderabad

3.**P. SAI KRISHNA** UG Scholar,
Department of CSE,
CMR Technical Campus,
Hyderabad

4.A.DIN REDDY
UG Scholar,
Department of CSE,
CMR Technical Campus, Hyderabad

ABSTRACT:-

Development of authorization mechanisms for secure information access by a large community of users in an open environment is an important problem in the ever-growing Internet world. In this paper, we propose a computational dynamic trust model for user authorization, rooted in findings from social science[8]. Unlike most existing computational trust models, this model distinguishes trusting belief in integrity from that incompetence in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different trusters. Simulation studies were conducted to compare the performance of the proposed integrity, belief model with other trust models from the literature for different user behavior patterns. Experiments show that the proposed model achieves higher performance than other models, especially in predicting the behavior of unstable users.

Keywords:- *Role-Based Access Control (RBAC), Mcknight"s Trust Model, Computational Trust Models.*

1.INTRODUCTION:-

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. However, holding evidence does not necessarily certify a user's good behavior. For example, when a credit card company is deciding whether to issue a credit card to an individual, it does not only require evidence such as social security number and home address, but also checks the credit score, representing the belief about the applicant, formed based on previous behavior. Such belief, which we call dynamic trusting belief, can be used to measure the possibility that a user will not conduct harmful actions. In this work, 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. Empirical evaluation supports that the distinction between competence and integrity trust is necessary in decision-making[13]. In many circumstances, these attributes are not equally important. Distinguishing between integrity and competence allows the model to make more informed and fine-grained authorization decisions in different contexts. Some real-world examples are as follows:

1) On an online auction site, the competence, trust of a seller can be determined by how quickly the seller ships an item, packaging/item 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 consent. In the case of an urgent purchase, a seller with low integrity, trust can be authorized if he/she has high competence [4] trust.

2) For an online travel agency site, competence consists of elements such as finding the best car deals, the best hotel deals, the best flight deals etc., whereas integrity trust is based on factors like whether the site puts fraudulent charges on the customers' accounts. 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.

3) For 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 un trusted parties While government agencies would usually prefer high integrity in web services, high-competence ervices with low integrity could be authorized for real-time missions. Experimental evaluation of the proposed integrity belief model in a simulated environment of entities with different behavior patterns suggests that the model is able to provide better estimations of integrity trust behavior than other major trust computation models, especially in the case of trustees with changing behavior.

2. IMPLEMENTATION MODULES:-

1. Mcknight's Trust Model
2. Computational Trust Models
3. Context and Trusting Belief
4. Belief information and reputation Aggregation methods

Mcknight's Trust Model:-

The social trust model, which guides the design of the computational model in this paper, was proposed by McKnight et al. after surveying more than 60 papers across a wide range of disciplines. It has been validated via empirical study. This model defines five conceptual trust types: trusting behavior, trusting intention, trusting belief, institution-based trust, and disposition to trust. Trusting behavior[8] is an action that increases a truster's risk or makes the truster vulnerable to the trustee. Trusting intention indicates that a truster is willing to engage in trusting behaviors with the trustee. A trusting intention implies a trust decision and leads to a trusting behavior.

Two subtypes of trusting intention are:

1. Willingness to depend: the volitional preparedness to make oneself vulnerable to the trustee.

2. Subjective probability of depending.

Computational Trust Models:-

The problem of establishing and maintaining dynamic trust has attracted many research efforts. One of the first attempts trying to formalize trust in computer science was made by Marsh[13]. The model introduced the concepts widely used by other researchers such as context and situational trust. Many existing reputation models and security mechanisms rely on a social network structure[1] . Propose an approach to extract reputation from the social network topology that encodes reputation information. Walter et al. propose 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. Lang[9] proposes a trust model for access control in P2P networks[2], 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.

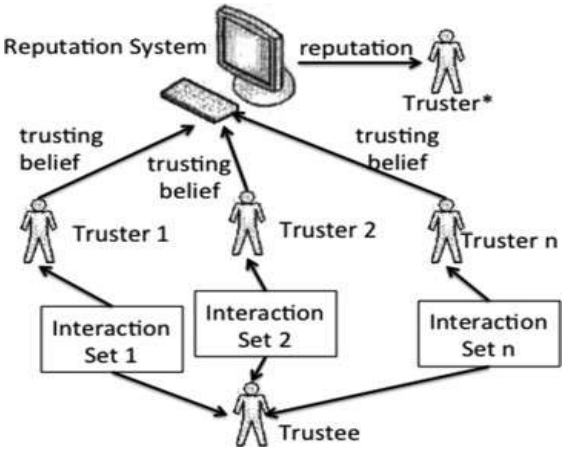
Context and Trusting Belief:-

Context: Trust is environment-specific . Both trusters concern and trustees' behavior vary from one situation to another. These situations are called contexts. A truster can specify the minimum trusting belief needed for a specific context. Direct experience information is maintained for each individual context to hasten belief updating. In this model, a truster has one integrity trust per trustee in all contexts. If a trustee disappoints a truster, the misbehavior lowers the truster's integrity belief in him. For integrity trust, contexts do not need to be distinguished.Competence trust is context-dependent. The fact that Bob is an excellent professor does not support to trust him as a chief. A representation is devised to identify the competence type and level needed in a context.

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.

3.SYSTEM ARCHITECTURE:



4. OPERATIONS DEFINED ON TRUST MODEL :

This segment presents the operations defined on the trust model.

1. **Building and testing trusting beliefs** Differenttechniques 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.

2. **Building and testing initial competence trust:** There arefour 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 withsome 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.

CANDIDATE METHOD SET TO BUILD INITIALCOMPETENCE 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.

5. ALGORITHM:-

To Build/Test Initial Competence Trusting Belief:-

input: t1, u1, c, δc, δp
Output : true/false
unusedMS := candidate method set in Table 1 defined
i := 1
M := the applicable method with highest priority
result[i] := compute($TC^{v}_{t1\rightarrow u1}(c)$, $TC^{P}_{t1\rightarrow u1}(c)$)using
MtestResult := 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)

6. CONCLUSION:-

In this paper we presented a dynamic computational trust model for user authorization. This model is rooted in findings from social science, and is not limited to trusting belief as most computational methods are. We presented a representation of context and functions that relate different contexts, enabling building of trusting belief using crosscontext information. The proposed dynamic trust model enables automated trust management that mimics trusting behaviors in society, such as selecting a corporate partner, forming a coalition, or choosing negotiation protocols or strategies in e-commerce. The formalization of trust helps in designing algorithms to choose reliable resources in peer-to-peer[3] systems, developing secure protocols for ad hoc networks and detecting deceptive agents in a virtual community. Experiments in a simulated trust environment show that the proposed integrity trust model performs better than ther major trust models in predicting the behavior of users whose actions change based on certain patterns over time.

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. 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 and Secure Computing, vol. 9, no. 2, pp. 261- 274, Mar./Apr. 2012.

[4] C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," Proc.Second ACM Conf. Electronic Commerce, pp. 150-157, 2000.

[5] L. Fan, "A Grid Authorization Mechanism with Dynamic Role Based on Trust Model," J. 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 Comm. Surveys, vol. 3, no. 4, pp. 2-16, Fourth Quarter 2000.

[7] J.D.Hamilton, TimeSeriesAnalysis. PrincetonUniversity Press, 1994.

[8] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," Proc. IEEE Ninth Int"l Conf. Young Computer Scientists (ICYCS „08), pp. 1963- 1968, 2008.

[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," Proc. Int"l Conf. Computational Intelligence and Software Eng. (CiSE), pp. 1-4, 2010.

[11] X. Long and J. Joshi, "BaRMS: A Bayesian Reputation Management Approach for P2P Systems," J. 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," Proc. Second Int"l Workshop Intelligent Systems and Applications, pp. 1-4, 2010.

[13] S. Marsh, "Formalizing Trust as a Concept," PhD dissertation- Dept. of Computer Science and Math., Univ. of Stirling, 1994.

Author's Profile:

1.T.Vineetha, Presently Pursuing B.Tech.,CSE in CMR Technical campus, Hyderabad, Telangana, INDIA. Her interesting domains are Network Security, Cloud Computing, Image Processing,etc. 2.Regonda.Nagaraju presently working as an Associate Professor in CMR Technical campus, Hyderabad, Telangana, INDIA. He received his M.Tech (CSE) degree from JNTU Hyderabad in the year 2011.He received B.Tech. (CSE) degree from JNTU Hyderabad, in the year 2006. His interesting domains are Image Processing, Machine learning, Network Security, Cloud Computing, Internet of Things(IOT) ,etc.

3.P.Sai Krishna presently Pursuing B.Tech.,CSE in CMR Technical campus, Hyderabad, Telangana, INDIA. Her interesting domains are Network Security, Cloud Computing, Image Processing,etc
4.A.Din Reddy presently Pursuing B.Tech.,CSE in CMR Technical campus, Hyderabad, Telangana, INDIA. Her interesting domains are Network Security, Cloud Computing, Image Processing,etc