The Strong Confidence: The Process of Computational Dynamic Trust Model for Secure Communication in Multi-Agent Systems

[1]Mrs.Joshi Padma Narasimhachari, [2]Valli Kumar Masam,[3]Dr. N. Ravi Shankar,[4]Dr. M. B. Raju
[1]Associate Professor,Head Of the Department,CSE, Sreyas Institute of Engineering & Technology,
padmajoshi2015@gmail.com
[2]PG Scholar, Department of CSE, Sreyas Institute of Engineering & Technology, mvallikumar@gmail.com
[3]Professor, Department of CSE, Lakireddy Balreddy College of Engineering, Vijayawada .ravish00@yahoo.com
[4]Professor, Department of CSE, KrishnaMurthy Institute of Engineering & Technology, Hyderabad.
drrajucse@gmail.com

ABSTRACT:

The license for development of mechanisms for information security across a wide range of users in open environment is an important factor in the growing world of Internet problem. In this article the confidence of a dynamic user permission model For calculations is proposed, and rooted in the results of the social sciences. Unlike most existing trusted computational models, and this model distinguish estrusting integrity belief that in the jurisdiction in different contexts, and represents oneself in evaluating and particular trustee different Trusters. Simulation studies to compare the performance model believes the proposed security trustee with other forms of literature for the various patterns of user behavior made. Experiments show that the proposed model achieves higher performance other models, especially in predicting the behavior of users uncomfortable.

1.INTRODUCTION:

In a multi-agent system agents interact with each other To achieve a specific goal that can not achieve alone [1] These include P2P [2-5] systems, grid computing [6] and the Semantic Web [7], and deployed computing [8] Network intrusion. The multiagent systems (mass) are increasingly It became popular in the realization of high value and guaranteed data Across the network. However, the open and dynamic MAS has made the nature of a challenge for researchers MAS to work in a secure environment for information business process. malicious agents who are always looking for ways to Exploit any weakness in the network. Is Where trust and reputation play a crucial role in ensuring effective interactions between the actors involved [9, 10]. Researchers have long to take advantage of the theory of trust The social network to build confidence for effective models Malignant behavior suppression agents involved. Issues are becoming more and more popular as confidence Traditional approaches to network security, such as the use Wall firewalls, access control and issuing certificates can not be authorized Predicting the behavior of agent from the point of view of "trust". reputation-based model [11-14] Trust collects, distributes, and aggregates feedback about previous participants Behavior. These factors help determine models of them safely, Promoting a trustworthy behavior, and inhibition of post Before the agents who are dishonest. trust based on reputation The models are mainly divided into two parts on the basis of the class The information is compiled and means from the perspective of a resident [15,16]. They are "a direct / local model experiment" and when direct "universal model / indirect reputation" experience It is derived from interviews or direct observation (first part Experience) reputation is a direct derivative of inferences Based on the information that has been collected indirectly (negative Evidences as word of mouth). Therefore, in the case of models reputation worldwide [17-29] agent added Feedback from all agents that interact with each time Agent goal of any agent having a view of the network It is wider than its own experience, which allowed A converge quickly to a better decision. However, the global reputation models are more difficult to manage Models of local experience as malicious agents Opportunity to provide false feedback. Most current models can successfully worldwide reputation Isolate malicious agents when the agents acting predictably. However, these models suffer both When agents begin to show any dynamic personality when They begin to act in a way that benefits them. These The models also failed to adapt to the sudden change agents " Behavior and as a result suffer when they alter their agents Strategic activities. Moreover, some models 2 It is mentioned in the treatment of complex attacks, as the impact Classification of dishonest or unfair collusion. Other aspect It slowly became important for proper maintenance The quality of service is adequate distribution Work load among the suppliers of reliable services. With out Salim load balancing scheme in high reputation And service providers would be enormous and ultimately Cause a bottleneck in the quality of service system. to the It's better than nothing. We need to know the confidence of existing models Given the balance between service providers. With these problems in mind research, we suggest Reactions to account base called dynamic trust model SecuredTrust that can detect sudden effective strategy A change in the malicious behavior with an additional Workload among providers of property services balance. SecuredTrust considers a number of factors in determining trusted agent such as satisfaction, similarity and reactions Last credibility and trust, the historical sudden deviation and confidence The erosion of trust and confidence. We have used a new policy for the Using the average exponential function storage reduction top agents in the trust account. We also have a new balancing algorithm is proposed based on approximate Calculate the size of the current work in the different services providers.

EXISTING SYSTEM:

- Many existing reputation models and security mechanisms rely on a social network structure.
- Pujol et al. 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 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.

DISADVANTAGES OF EXISTING SYSTEM:

- 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.
- The existing approaches do not consider "context" as a factor affecting the value of trust,which prevents an accurate representation for real life situations.

PROPOSED SYSTEM:

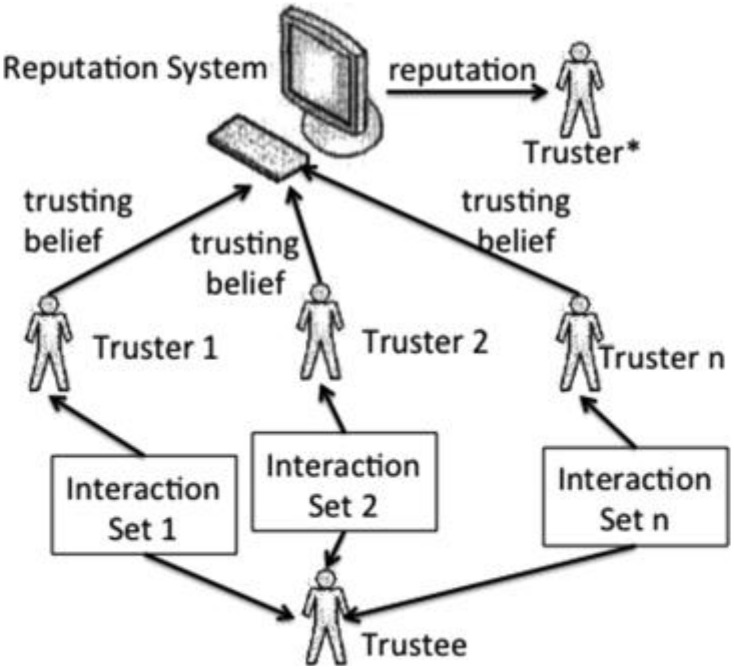
- In this work, we propose a computational dynamic trustmodel for user authorization. Mechanisms for buildingtrusting belief using the first-hand (direct experience) aswell as second-hand information (recommendation andreputation) are integrated into the model. The contributionsof the model to computational trust literature are:

- ❖ The model is rooted in findings from social science,i.e., it provides automated trust management thatmimics trusting behaviors in the society, bringing trust computation for the digital world closer to theevaluation of trust in the real world.
- ❖ Unlike other trust models in the literature, the proposedmodel accounts for different types of trust.Specifically, it distinguishes trusting belief in integrityfrom that in competence.
- ❖ The model takes into account the subjectivity of trustratings by different entities, and introduces a mechanismto eliminate the impact of subjectivity in reputationaggregation.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ Distinguishing between integrity and competence allows the model to make more informed and fine-grained authorization decisions in different contexts.
- ✓ The trust model we propose in this paper distinguishesintegrity trust from competence trust.

SYSTEM ARCHITECTURE:



Implementation Modules:

1. **Mcknight's Trust Model**
2. **Computational Trust Models**
3. **Context and Trusting Belief**
4. **Belief information and reputationAggregation 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* 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. 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 . 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 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.

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.

CONCLUSION:

In this work, we have confidence in computational bio Model for the user's permission. This model has its roots in findings of Social Sciences, and not limited to trusts When the belief that most of the computational methods are. we did The context and functions that relate to different representation Contexts, able to build trust with the belief cross context Information. Trust dynamic model proposed allows automated trust administration, which mimics the behavior of confidence in the community, Such as the choice of partner companies, and the formation of a coalition government, or Choose to negotiate protocols or strategies in the field of electronic commerce. The formalization of trust helps in the design of algorithms for Choose reliable resources in the peer to peer systems, and development of secure protocols dedicated to networks revealed misleading agents in a virtual community. Experiences Exposure simulation trust security environment proposed Confidence outperforms other major forms of trust model To predict the behavior of users who change procedures 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.

[14] P. Matt, M. Morge, and F. Toni, "Combining Statistics and Arguments to Compute Trust," Proc. Ninth Int'l Conf. Autonomous Agents and Multiagent Systems (AAMAS '10), pp. 209-216, 2010.

[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, Sept. 2002.

[16] D. McKnight and N.L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationship Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS '01), 2001.

[17] W. Mendenhall and R.J. Beaver, Introduction to Probability and Statistics. PWS-Kent Publishing Company, 1991.

[18] A. Nagarajan and V. Varadharajan, "Dynamic Trust EnhancedSecurity 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," Proc. Int'l Conf. Autonomous Agents and Multiagent Systems (AAMAS '02), pp. 467-474, 2002.

[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.

AUTHOR'S PROFILE:

Mrs.Joshi Padma Narasimhachari
Associate Professor,Head Of the Department,CSE, Sreyas Institute of Engineering & Technology, padmajoshi2015@gmail.com

Valli Kumar Masam
PG Scholar, Department of CSE, Sreyas Institute of Engineering & Technology, mvallikumar@gmail.com