INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A COMPUTATIONAL MODEL WITH TRUSTING BELIEF AND SECURITY: LITERATURE REVIEW

G. P. BABHULKAR[1], PROF. MS. V.M. DESHMUKH[2]

1. Persuing Master of Engineering, Dept. Of information Technology, Prof. Ram Meghe Institute of Technology and Research, Badnera-Amravati-444701, Maharashtra.
2. HOD, Dept. Of Information and Technology, Prof. Ram Meghe Institute of Technology and Research, Badnera-Amravati-444701, Maharashtra.

Accepted Date: 13/12/2015; Published Date: 01/01/2016

Abstract: - The users of internet are growing vastly because of its ease in social life but secure information access in open environment with trust by large community is ever growing problems. In this paper we put an opinion about security and trust of computational model by studying and analysing various computational models according to its characteristics based on security and trust. All the models which we are studied, some are one directional and some are bidirectional. We tried to collect various features of various models so that one computational model should be formed which provide better security and trust among truster/(s) and trustee/(s). It helps to maintain security and trust between truster and trustee.

Keywords: Trust model overview, Security

Corresponding Author: MR. G. P. BABHULKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

G. P. Babhulkar, IJPRET, 2015; Volume 4 (5): 76-81

PAPER-QR CODE

INTRODUCTION

the everyday increasing wealth of information available online has made a problem. so, secure information access mechanism is very important, so that the user can keep trust on trustee. development of authorization mechanisms for secure information access and maintaining the trust by a large community of users in an open environment is an important problem.

the modern system uses digital identity to validate users. however, the digital evidence cannot certify the user's behavior is good or bad. for example, when user applies for loan then bank checks not only address, salary, etc. but also last six months' statement and income tax return file. by using statement and tax document, bank can identify the behavior of that user and decide loan amount. such belief is called dynamic trusting belief, can be used to determine the possibility that the user will not conduct harmful action and bank does not require to face any problems in future.in this work, we reviewed the different a computational trust model to create single model which provide better security and create trust.

LITERATURE REVIEW

McKnight's Trust Model

McKnight proposed the computational model to develop the social trust [1]. 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 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: the likelihood that a truster will depend on a trustee.

Trusting belief is a truster's subjective belief in the fact that a trustee has attributes beneficial to the truster. The following are the four attributes used most often:

1.Competence: a trustee has the ability or expertise to perform certain tasks.

2.Benevolence: a trustee cares about a truster's interests.

3.Integrity: a trustee is honest and keeps commitments.

4.Predictability: a trustee's actions are sufficiently consistent.

Institution-based trust is the belief that proper structural conditions are in place to enhance the probability of achieving a successful outcome.

Two subtypes of institution-based trust are:

1.Structural assurance: the belief that structures deployed regulations, promises etc. promote positive outcomes. Structures include guarantees, policies etc.

2. Situational normality: the belief that the properly ordered environments facilitate success outcomes.

Disposition to trust characterizes a truster's general propensity to depend on others across a broad spectrum of situations. Two subtypes of disposition to trust are:

1. Faith in human: the assumptions about a general trustee's integrity, competence, and benevolence.

2. Trusting stance: a truster's strategy to depend on trustees despite his trusting belief about them.

Trust intention and trusting belief are situation and trustee specific. Institution-based trust is situation specific.Disposition to trust is independent of situation and trustee. Trusting belief positivey relates to trusting intention,which in turn results in the trusting behavior. Institution-based trust positively affects trusting belief and trusting intention. Structural assurance is more related to rusting intention while situational normality affects both. Disposition to trust positively influences institution-based trust, trusting belief and trusting intention. Faith in humanity impacts trusting belief.

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 [2]. 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 [3]. Pujol et al. propose an approach to extract reputation from the social network topology that encodes reputation information [19]. Walter et al. [4] 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 [5] 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. Similarly, Long propose a Bayesian reputation calculation model for nodes in a P2P network, based on the history of interactions between nodes.

Trust value structure

In trust model decision can be taken on the basis of trust value as shown in figure1

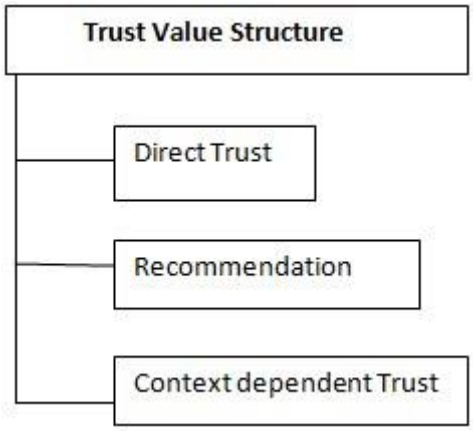

Fig.1 Trust Value Structure

Direct trust between two entities is formed on the basis of previous interactions and a part of overall trust value in the majority of trust model developed. **The recommendation trust** is based on the reputation of the trusted entity. Reputation trust is the strongest value because the reputation cannot create easily in the market. It takes longer time to achieve, so any one can easily keep faith on such organization. The Situational trust is depending on situation so it is dynamic and it is evaluated on the basis of the current situation.

The direct trust between two entities is mainly formed as a result of their previous interactions and is a part of the overall trust value in the majority of the trust models developed so far. However, the models differ in the method how the direct trust value is calculated. The model proposed by Song specifies a prior job success rate, firewall capabilities, anti-virus capabilities and capabilities of intrusion detection system as a part of the final direct trust value. In the model proposed by Azzedin and Maheswaran the direct trust is evaluated according to the behaviour of the evaluate dentity, which is expressed as the willingness to abide requirements

declared by the trusting entity and any violation of these requirements leads to a penalty in the direct trust. The recommendation trust is referred to as a reputation of the trusted entity and can be described as everything that is generally said or believed about the entity's character or standing. If the trusting entity is aware of the trusted entity's reputation it can base its

trust on that reputation, i.e. the trusted entity is trusted because of its good reputation. On the other hand, if the trusting entity has a private knowledge about the trusted entity (e.g. through direct experience) and the private information overrules any reputation the trusted entity might have, then the trusted entity can be trusted despite

its bad reputation. Entities reveal and obtain reputation for the purpose of a decision making in several ways. The model proposed by Ding calculates the overall trust value according to the recommendation trust among VOs instead the grid entities. The reason for this approach is the fact that the number of VOs is smaller than the number of grid entities. Hence, the reputation can be managed in a more scalable manner. The model proposed by Ryutov et al. monitors behaviour of entities and if some action on one grid entity is regarded as insecure, the same behaviour is likely to be insecure to other similar entities as well. Therefore, the grid entities distribute warnings to other entities as soon as a threat was detected.

Table 1: Comparison of Trust Models

Trust Models	Approach of Models	Trust Origion	Trust relationship
Lin et al. [13]	Linear combination	From reliability and competence of users	Bidirectional i. e. trust of entity depends on context.
Kumar and Ramchandram [20]	Fuzzy logic	From availability and reliability of the source	One directional i. e. User's point of view
Song et al. [17]	Fuzzy logic	From behavior of past action	One directional
Azzedin and Maheswaran [6]	Linear Combination	From past behaviour in the past collaboration	Bidirectional
Kaur and SenGupta[9]	Linear combination	Behaviour in past collaboration and its characteristics.	One directional.
Bharat Bhargav and Pelin Angin[7]	User Authorization	From context trust	One directional

Description of Models:

The model proposed by Azzedin and Maheswaran[6] to manage trust on two criterion. One is identity trust and behaviour trust. Identity trust is depends on identity of user and its behaviour. Song et al. is depends on user's own security and reputation obtained from past history. The main disadvantages of this model is that trust was obtained according to users. The Bharat Bhargav and Pelin Angin's model is based on integrity and contextual trust.

CONCLUSION

The purpose of the this review paper is to study various models and try to gather all advantages which are present in various model to develope a strong model which provides security and trust between truster and trustee.

REFERENCES

1. McKnight and N.L. Chervany," Conceptualizing trust: a typology and e-commerce customer relationship model" In Proc. HICS34,2001.

2. S. Marsh, "Formalizing Trust as a Concept," Ph.D. dissertation, Dept. Comp. Science and Math., Univ. Stirling, U.K., 1994.

3. 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.

4. 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.

5. B. Lang, "A Computational Trust Model for Access Control in P2P," Science China Information Sciences, vol. 53, no. 5, pp. 896-910, May, 2010.

6. F. Azzedin and M. Maheswaran. evolving and managing trust. In Canadian Conference on electrical and computer engineering,2002.

7. Bharat Bhargav and Pelin Angin "A Computational Dynamic Trust Model for User Authorization", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL.12