Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 527 – 534

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

A Survey of Trust Models for Enterprise Information Systems

Asmita Manna[a,*], Anirban Sengupta[a], Chandan Mazumdar[a]

[a]*Centre for Distributed Computing, Dept. of Computer Science and Engineering, Jadavpur University, Kolkata-700032,India*

Abstract

Most of today's enterprises are open in a competitive market worldwide and dependent on distributed information infrastructure across various geospatial location and various cyber spatial location as well with a purpose of offering ready and effective services to customers. But this decentralization comes at the cost of security. The distributed computing framework is vulnerable to attacks from malicious agents, thereby increasing the chances of risks and security breaches. Trust and Reputation management system is a tool to combat security threats. A trust management system helps its user to decide how trustworthy the other party is before making a transaction. This work aims to identify the required characteristics of trust needed for an enterprise network and presents a survey of a few well known trust models with an aim to identify trust characteristics in each model.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Trust Model, Enterprise Information System

1. Introduction

From social science perspective, trust is an essential parameter for any type of transaction among human beings. Additionally, trust is also needed for all automated information processing systems. In computer science research, formal studies on trust and reputation have been undertaken in various areas like security and access control, reliability and robustness of distributed systems, and policies for decision making under uncertainties, particularly in the area of e-commerce. However, in the domain of Enterprise Information System (EIS), trust is a relatively new paradigm. In case of enterprise information systems, notion of trust has only been considered in credential checking for access controls. But, in today's scenario, when enterprises are open in a competitive market worldwide with a major share in open systems like internet and cloud, they are more vulnerable to attacks. To make enterprises more secured and attack-resilient, trust values of different stakeholders should be considered before allowing any kind of

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.212

transaction or information communication. Most of the existing credential-based trust models do not consider the past behavior or reputation of a stakeholder; experience-based trust models do not differentiate among different contexts of trust evaluation; most social science models cannot evaluate trust in a measurable form; distributed system trust models only focus on aspects of secure communication. It can be seen that there is not a single available trust model which can cater to the different requirements of EIS, while being compatible with existing security policies of the enterprise. In this paper, a survey of available trust models based on required and identified attributes is presented. The paper looks at the pros and cons of the models with an aim to enable researchers to develop a comprehensive trust model for EIS that will be able to generate useful and usable security policies. The rest of the paper is organized as follows. Section 2 defines the need of trust evaluation from EIS perspective; Section 3 defines the taxonomy of trust and reputation; Section 4 discusses about required attributes of trust model; Section 5 presents a brief description of models and a table showing the comparison of different trust models; finally, Section 6 concludes the paper.

2. Need of trust evaluation for enterprise

According to current enterprise information system scenarios, users can be divided into three categories: organizational personnel, customers and visitors. Among them, organizational personnel directly interact with the IT and non-IT resources of an enterprise; hence, they have the maximum opportunity of misusing the systems. Personnel, with only a minimum level of trust value, should be allowed access to the EIS. But those values must not be static; instead they should evolve with time, based on their interaction with the system. To assign the trust value for first time, EIS has to heavily rely on credentials and background checking.

Customers are the most important users and the basic goal of the enterprise should be to satisfy customers. They are exposed to only a small portion of EIS resulting in very little chance of harming the system physically. However, dissatisfied customers can harm the intangible assets of an enterprise. Particularly in today's virtual world, a customer's feedback and thoughts can easily be propagated to others in no time. So, to protect its reputation and goodwill, an enterprise cannot afford to allow erroneous feedback; there lies the usage of trust evaluation for customers.

Visitors are neither exposed to resources, nor do their feedback carry much value for an enterprise. That is why not many precautions are taken regarding visitors, leaving them with a probability of harming the enterprise in an unexpected way. So there must be a trust value evaluation for each visitor before permitting him/her in the enterprise's physical premises or virtual premises as well. Credential-based trust evaluation is the basic manner of trust value evaluation of a visitor.

3. Taxonomy of trust models

There has been a lot of research related to trust evaluation in computer science. They can be classified into three major categories:

a. Credential-based trust: Credentials are testimonials or certified documents showing the qualification or status of an individual that entitles him to certain services and powers. Here it is assumed that trust is established by verifying certain credentials and once trust is established, access rights to different resources are granted using pre-defined policies. These are widely used in access control.

b. Reputation-based trust: Reputation is nothing but the cumulative knowledge about past behavior of an entity and relevant events and interactions of the entity with an agent. Based upon that knowledge, it is predicted how that entity will behave in future. This knowledgebase can be created in two ways: direct experience of truster or, if direct interaction is not available, recommendation from other agents can be taken into account. The complexity associated with recommendations is high because it introduces uncertainty, as recommenders can manipulate or conceal parts of true information for their own benefit, leading to the breakdown of the Trust and Reputation model. These models even compute trust over a social relationship or across a third-party recommender based path. Reputation, either via direct trust or recommended trust, forms the core of trust modeling in general.

c. Trust in information resource:

In both credential-based and recommendation-based system, the basis of trust formation starts with a known attribute; either credential which is ideally provided by a trusted organization or by past behaviors, either judged by truster itself or based on others' interactions. However, in web-based information systems, these third parties

working as recommenders may not be trusted or their identities can easily be compromised. Thus for web-based systems, a hybrid model of credential-based and reputation-based model should be used.

4. Attributes of trust model

a. Context dependency

Context is a set of information that can be used to characterize the environment of an entity. Trust is **context dependent**. It means, for a particular entity, trust value may change if the context is different.

$$AT(c_i)B \not\Rightarrow AT(c_i)B, where\ i \neq j$$

For example a software company can trust a particular employee for following the proper coding paradigm in building the software but it cannot trust him in the context of submitting tender for a new contract. In an enterprise, a single user can have different roles at different times. Separation of duties (SoD) is an essential criterion in organizational structure. Context-dependency helps in better implementation of SoD with respect to trust.

b. Non transitivity

Transitivity is a property which says that if an element a is related to an element b, and b is in turn related to an element c, then a is also related to c. Given, that a~b and b~c, then the transitive property tells us a~c where "~" means "relates to".

Trust is not transitive – all evaluations of recommendations take into account the source of the recommendation. For example, if Alice trusts Bob and Bob trusts Cara, it does not necessarily follow that Alice must trust Cara by any degree. In some cases, trust is considered as **conditionally transitive** which says that if A trusts B and B trusts C, then A also trusts C with the condition that B acts as a recommender to C based on C's reputation.

In some cases, trust is considered as **partially transitive** which means if A trusts B and B trusts C for a particular context, then this chain relationship creates a partial trust value for A on C.

$$\forall C_i(AT(C_i)B = \alpha) \wedge (BT(C_i)C) = \beta \Rightarrow AT(C_i)C = f(\alpha, \beta)$$

where **i** = 1…k , **α** indicate the trust value of A on B and **β** indicate the trust value of B on A.

This is important because in enterprise network, recommendation plays an important role in trust evaluation where manipulation based on professional rivalry can take place. Thus partial transitivity and conditional transitivity are two important aspects to consider. Conditional transitivity is later elaborated as Hierarchy of trust.

c. Non monotonicity

An enterprise scenario is dynamic in the sense that it deals with new customers, adds more functionalities and personnel to its EIS continuously. Interaction among different stakeholders of an enterprise may generate experiences of different satisfaction levels. If trust is considered monotonic, each experience cannot be judged properly based on latest interaction. So, trust is considered non-monotonic which never increases or decreases consistently; it evolves based upon satisfaction level of latest interaction.

Here,

$$D(AT(c_i)B)$$

implies direct trust of A on B for context c_i and μ indicates the satisfaction level for the latest interaction.

d. Subjectivity

Subjectivity is a subject's personal perspective, feelings, beliefs, desires or discovery, as opposed to those made from an independent, objective point of view. In case of EIS, trust is evaluated from objective point of view for most of the contexts but still for some contexts, subjectivity should be considered. Particularly for customer feedback, subjectivity is important because different customers' expectations may vary, especially where no SLA is specified.

While building the Trust model for first time, subjectivity must be considered as an attribute of a general trust model. Later the model may be refined to reduce the subjectivity factor for an enterprise at the time of customization and adaptation of the base model for a particular enterprise.

e. Uncertainty

Uncertainty is the quality, state or situation where the current state of knowledge is such that (1) the order or nature of things is unknown, (2) the consequences, extent, or magnitude of circumstances, conditions, or events is unpredictable, and (3) credible probabilities to possible outcomes cannot be assigned. With respect to Enterprise information system scenario, uncertainty is important in trust evaluation because in many cases, the number of interactions among stakeholders and the enterprise is limited; therefore the nature of things is unknown and possible outcomes cannot be guessed. This is particularly applicable when an enterprise is dealing with stakeholders who do not interact much with the enterprise, but have an influence on major decisions.

f. Asymmetry

A relation is called **asymmetric** if every time the relation holds from A to B, it does not also hold from B to A. In general, if node A trusts another node B, that does not necessarily indicate that B also trusts A.

$$ATB \not\Rightarrow BTA$$

where A*T*B = Average overall trust value of A on B and B*T*A = Average overall trust value of B on A. Even if both A and B trust each other, that does not necessarily indicate the trust value of A on B (α) equals the trust value of B on A (β) or A trusts B's level may be not same as B trust A's level. If we delve a bit more and expand on this property about a specific context c_k where A$T(c_k)$B indicates the trust of A on B for context c_k, then all the above statements also hold. If both A and B have the same context c_k (for example we can think of service-date and time sharing) to offer, then A$T(c_k)$B indicates a high probability for B$T(c_k)$A. These conditions make trust **non-antisymmetric**.

$$ATB = \alpha \wedge BTA = \beta \not\Rightarrow A = B$$

where α, β may or may not be equal. Trust is very much context dependent. Now, as in most cases, enterprise and its stakeholders do not judge each other on the same context. Thus, trust is considered non symmetric or anti-symmetric.

g. Temporal decay

Enterprise Information Systems are highly dynamic; hence, the basic trust value w.r.t a defined context should not be static. If interaction happens, trust value may be re-evaluated but if there is no interaction, trust value should follow the natural law of depreciation just like any other asset. As time progresses, an entity's reputation with respect to other entities changes to an unknown state if little or no interaction occurs between them, meaning that reputation information is lost with time. Agent A may trust agent B at time t1 and may not trust it any more at time t2. It is important to have the reputation of an entity (whether good or bad) converge to a neutral value as time passes by and no interactions take place. Thus, no reputation lasts forever.

$$c_i((AT(c_i)B)t > (AT(c_i)B)t + \Delta t) \wedge \text{no new interaction, where } i = 1,...,k$$

h. QoS Monitoring

An enterprise is created for business ventures. Providing quality services within stipulated time is a major concern for an enterprise. Thus same objective measurement should be used for evaluating trust too. Intuitively, if the quality of a service can be objectively measured, then an entity's trustworthiness for that service reflects some intrinsic property of that entity, which should be independent of the source of the trust evaluation. Some QoS attributes can actually be measured by some engines during transactions. For example the response time, availability, etc. proposes to assess the reputation of web services based on the attribute compliance – the difference between the projected and the delivered values of quality. Trust based on QoS monitoring is especially useful when users' ratings suffer from

common problems, for example dishonest rating, spamming, etc. In reality, different service domains have different sets of QoS and different service consumers are also interested in different QoS. When selecting a service, consumers want to know the reputation of the web-service in different QoS. Besides QoS or Objective measurement, subjective measurements should also be considered while developing trust model because QoS does not provide a holistic view of user's satisfaction.

i. Hierarchy

The past behavior of an entity is one of the major attributes for trust calculation. Recommendation plays an important role in judging an entity on its past interactions. But every recommendation should not be given equal weightage while evaluating trust. The credibility of recommender should be checked first and **hierarchy of trust** should be considered. Reputation of an entity should be considered hierarchically; that means the circle of friends with whom the truster has more interactions should be given more weightage than those having little or no interaction at all. For enterprise information system, hierarchy of trust is very important.

j. Feedback credibility

Credibility is the degree to which a communicator or communication is believed by the recipient. Credibility is important when the message to be transmitted and interpreted is not in line with the idea or belief possessed by the receiver. The credibility of a message has a higher value if it is delivered by a trustworthy and reliable transmitter. This attribute deals with the confidence in a transmitter's reliability and consistency in giving trusted advice and suggestion. For feedback based trust evaluation system of enterprise, dishonest feedback should be differentiated from honest ones. The number of feedbacks provided by an entity, the pattern of feedback, longevity of entity's existence etc. play crucial role in identifying dishonest feedbacks.

k. Feedback similarity

For a feedback-based trust evaluation system, feedback similarity checking, i.e. how similar the feedback qualities are for two different entities, is important too. Similarity helps an enterprise to better classify entities into different groups. The similarity of an entity with another entity is based on the similarity of their reputation values. If reputation values of two entities are similar, it may be assumed that their evaluation procedure is almost similar. So, one entity's recommendation will be more credible to the other entity.

l. Credential validity

When there is little interaction history between the peers in an environment, the trust decisions can be made by the help of credentials and thus trust value with higher accuracy can be computed. The trust models which are based on credentials in essence employ an accurate and static way to describe and process complicated and adaptive trust relationship.

5. Description of existing trust models

The TrustBAC model [1] extends the conventional role-based access control model with the notion of trust levels and thus incorporates the advantages of both the role based access control model and credential based access control models. Users are assigned to trust levels instead of roles based on a number of factors like user credentials, user behavior history, user recommendation, etc. Trust levels are assigned to roles according to organizational policies. Roles are assigned to permissions as in the traditional RBAC model. Changes in the trust level of user changes the roles that the user has in the system and thus the user's privileges. The system can define as many trust levels as it wants and can assign each level to a specific set of resources tied with a specific set of access privileges. This model is well suited for open systems like the Internet.

A. A. Rahman and S. Hailes [2] proposed a trust model based on the real-world and sociological characteristics of trust. It deals exclusively with beliefs about the trustworthiness of agents based on experience and reputational information. At any given time, the trustworthiness of a particular agent is obtained by summarizing the relevant subset of recorded experiences. This trust model helps users to identify trustworthy entities and gives artificial autonomous agents the ability to reason about trust. This model is designed to deal with the notions of trust and reputation in virtual communities (e.g. rating recommendations for book authors).

The major drawback of this model is it uses only four trust degrees and fixed weights are assigned to feedbacks; this may not reflect facts correctly.

In [3], the authors proposed a trust algebra and a trust evaluation algorithm aiming to solve generic trust propagation and trust inference in trust graph and presented a general trust model based on trust algebra. They also presented an information entropy to quantitatively measure trust. The trust algebra framework is shown to be flexible enough to express other trust models and their scheme is shown to be applicable in different computing environments because of the use of two abstract operators (and) of trust algebra. The first operator is used to compute indirect trust value along a single path in trust graph and the second operator is used to combine opinions across paths. These operators can be used in a general framework for solving trust inference problems. This model is well-suited for open computing environments such as Grid computing, ad hoc networks, and peer-to-peer systems as well as component system, etc when entities cooperate to fulfill a co-task and trust model.

The model presented in [4] is based on reputation-based trust model and it enables a peer to combine reputation and credential in order to cope with the situation when there is little interaction history about this peer. This model consists of three modules: reputation module, credential learning module and integrated module and based on the correlation of credential and reputation, it can derive credential trust adaptively, then combine the credential trust and reputation to get the overall trust value; hence, it can track the changes of the credential's character accurately and adaptively. This model is useful when there is little transaction history between the peers and suitable for dynamic, open, uncertain trust environments as well as reputation-based trust management systems.

The authors in [5] have proposed a Bayesian network trust and reputation model for web services that can overcome limitations of traditional web service trust models by integrating three different kinds of trust sources: user rating, QoS monitoring information and direct experience of the requester, thus addressing both subjective and objective view of web-service trust. These sources are then weighted to derive the final reputation of the web-service. This model can provide sound results to assess the trust and reputation of web-services.

The model in [6] is based upon reputation values, direct experiences, and trust in the credibility of a host to give recommendations, decay of information with time based on a dynamic decay factor, first impressions, similarity, popularity, activity, cooperation between hosts, in addition to a hierarchy of host systems. Here, the reputation value of a host is calculated based on its previous experiences and the gathered reputation values from other hosts, and then it is decided whether to interact with the target host or not. In this model, the authors differentiate between two types of trust (namely, trust in the competence of a host and trust in the host's credibility and consistency) that affect the final decision of a host regarding whether to interact with another target host or not. This model is designed to meet the needs of distributed computing environments.

Tundjungsari et. al. [7] proposed a trust model to overcome problems in group decision making. This model aims to assist a group consisting of diverse decision makers with diverse background and knowledge and varied preferences to make an optimal decision. In this model, trust value is calculated from direct interaction and reputational information and this value is stored and subsequently updated in the User Identity Database (UIDB) and Trust References Database (TRDB). This mechanism is apt in making a decision when several decision makers are involved. For instance, this model fits the bill while making a participatory group decision in urban planning in a rural area.

The trust model proposed in [8] accommodates the notion of different degrees of trust, identifies how to determine the trust value, and defines how trust changes over time. Here, trust is shown to be context-dependent and trust relationship is numerically represented using three components viz. experience, knowledge, and recommendation. These components are used to calculate the trust value which is essential for granting and/or denying access to a user. This trust model is suitable for use in pervasive computing environment.

M. M. Haque and S. I. Ahamed [9] proposed the first formal omnipresent trust model for pervasive computing, which can be used universally. This trust model is context specific and reputation-based and uses a recommendation protocol that provides a multi-hop recommendation capability and a flexible behavioral model to handle interactions. The model aids in sharing of resources in an ad hoc network of handheld devices in a pervasive computing environment. It provides a mechanism for handling multi-hop recommendations, considers contexts as vectors and deals with both time and distance-based aging of trust values.

The model by X. Tang and M. Chen [10] is a recommendation trust model based on reputation or credibility (i.e., RBRTrust Model) which takes into account the subjective and objective factors which impact trust. The model considers interactive scope, interactive time, interactive context, etc., through local trust, direct trust and recommendation trust to get the overall trust value. The authors provide a specific method to calculate the trust

value, and also describe the overall trust evaluation strategy.This model aims to solve the recommendation trust problems in interoperability environment.

EigenTrust [11] is one of the most popular reputation management models for P2P network till date. It computes the level of trust that a system places on a participant based on the normalized local trust vector of the participant and its eigenvector. It enables the reputation computation and establishment of a participant through direct experiences and feedbacks as well as indirect experiences obtained through its circle of "friends". Friends of a participant refer to those other participants with whom this participant has had direct or indirect interaction or transaction relationship. Participants connected by such transactional relationship form a collaboration network or "friendship" network. The major drawback of this model is that it fails in case some dishonest participants form a friendship network among themselves with presence of normal participants. Secondly, though it uses friendship network effectively, it assumes friendship propagates equally instead of weighted propagation.

Peertrust [12] is a dynamic P2P trust model for quantifying trustworthiness of peers in P2P network. It is a context-aware trust evaluation system and is able to differentiate dishonest feedbacks from original ones. It also considers time-decay and non-monotonicity of trust evaluation so that any participant, which was previously trusted but is currently giving malicious feedback, can also be identified. However a major drawback is it does not consider hierarchical trust propagation.

6. Conclusion

Based on identified attributes a comparison is presented in Table 1. Trust model plays a crucial role in designing trust policies for different fields like e-commerce, sensor network, pervasive computing and particularly for access control. Not much work has been done towards designing trust based security policies for enterprise information security for which choosing a suitable trust model is a crucial issue. In this paper we have identified all attributes that a trust model must have for being used by an enterprise information security system. But none of the available models support all of them. In future we aim to design a trust model which will support all the attributes mentioned here and can be used for enterprise information systems.

Table 1: Comparative study of different Trust Models on the basis of trust attributes

Models	**Attributes of Trust in Models**											
	Context dependency	***Non transitivity***	**Non monotonicity**	***Subjectivity***	***Uncertainty***	***Asymmetry***	***Temporal decay***	***QoS Monitoring***	***Hierarchy***	***Feedback credibility***	***Feedback Similarity***	***Credential validity***
[1]	X	X	X		X	-						X
[2]	X	X	X		X	X						
[3]					X	X						
[4]					X	X						X
[5]				X		X		X				
[6]			X				X					
[7]		+				X*	X					
[8]	X		X	X			X	X				X
[9]	X	++				X	X					
[10]	X	X		X		X	X	X				
[11]	X		X	X	X		X			X		
[12]	X		X		X	X	X	X		X	X	

Where X denotes Yes. - denotes No, + denotes partial transitivity, ++ denotes conditional transitivity and * denotes non-antisymmetry

References

[1] S. Chakraborty and I.Ray, TrustBAC- IntegratingTrust Relationships into the RBAC Model for Access Control in Open Systems, SACMAT'06, June 7–9, 2006, Lake Tahoe, California, USA
[2] A. A-Rahman and S. Hailes, "Supporting Trust in Virtual Communities", in *The 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, 2000.
[3] Y. Wenjhong, H. Cuanhe, W. Bo, W. Tong and Z. Zhenyu , "A General Trust Model Based on Trust Algebra", 2009 International Conference on Multimedia Information Networking and Security, IEEE Std. 10.1109/MINES.2009.226
[4] J. Gong, J. Chen,, H. Deng and J. Wang, "A Trust Model Combining Reputation and Credential", 2009 WASE International Conference on Information Engineering, IEEE Std. 10.1109/ICIE.2009.159
[5] H.T. Nguyen, W. Zhao and J. Yang, "A Trust and Reputation Model Based on Bayesian Network for Web Services", 2010 IEEE International Conference on Web Services, IEEE Std. DOI 10.1109/ICWS.2010.36
[6] A. Tajeddine, A. Kayssi A. Chehab and H. Artail, "A Comprehensive Reputation-Based Trust Model for Distributed Systems", IEEE 2005
[7] V. Tundjungsari, J. E. Istiyanto, E. Winarko and R. Wardoyo, "A Reputation based Trust Model to Seek Judgment in Participatory Group Decision Making", 2010 International Conference on Distributed Frameworks for Multimedia Applications (DFmA)
[8] S. Yin, Indrakshi Ray and Indrajit Ray, "A Trust Model for Pervasive Computing Environments", IEEE 2006
[9] M. M. Haque and S. I. Ahamed, "An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment"**,** 31st Annual International Computer Software and Applications Conference(COMPSAC 2007), IEEE 2007
[10] X. Tang and M. Chen, "Reputation-Based Recommendation Trust Model in the Interoperable Environment", IEEE 2011
[11] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks",In Proceedings of the 12th international conference on World Wide Web, pages 640–651.
[12] L. Xiong and L. Liu.," Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities" IEEE Transactions on Knowledge and Data Engineering, 16(7):843–857, 2004