A Closer Look on Conceptual Modeling of Trust to Develop TrustMan system

Simon Samwel Msanjila

Information and Communication Technology Department, Mzumbe University
Mzumbe, Morogoro, Tanzania

Abstract

Designing comprehensive trust models and mechanisms to address challenges related to mediating business oriented collaboration among organizations has become a fundamental focus of research on trust and particularly those focused on organizational Trust Management (TrustMan) Systems. Despite recent achievements from research addressing the modeling of trust, there are still insufficient generic and customizable models, mechanisms and tools to support emerging requirements on inter-organizational trust analysis. Most available model solutions supporting trust analysis are limited to: a specific application case (e.g. multi-agent systems), known actors (organizations or individuals), or domain of study (e.g. health domain). These solutions are also limited to some specific set of trust criteria applied to their development such as a small set of trust criteria for analysis of rational trust in organization. In this article we advocate that a large number of elements must be properly specified and modeled to comprehensively cover the trust objectives of organizations towards developing a supportive TrustMan system. This article analyzes and proposes three specific modeling formalisms that best represent trust relationships among organizations and presents some examples for those formalisms. It also analyzes classes of models of inter-organizational trust, namely: hard models, soft models and semi-soft models.
Key words: Trust elements, trust models, inter-organizational trust, collaborative networks, VO breeding environments, TrustMan system

1. Introduction

Considering the key role that trust plays in facilitating collaboration within collaborative network (CN) of organizations, the understanding of the base concepts relating to inter-organizational trust is necessary for creating sustainable collaborative networks of organizations. Conceptual modeling of trust relationships between organizations fundamentally contribute to creating a common understanding of inter-organizational trust among different actors. Modeling of trust in organizations aims at supporting the involved actors to enhance understanding of elements and concepts of trust towards achieving the trust objectives in the collaborative network of organizations. However, the needed models and the focus of learning might differ depending on the form of collaborative networks and the nature of interactions among member organizations. Two most popular forms of collaborative networks of organizations are mentioned and defined in [Camarinha-Matos & Afsarmanesh, 2006] as virtual organizations (VO) and VO breeding environments (VBE) as stated below:

Virtual Organization (VO) – represents an alliance comprising a set of (legally) independent organizations that share their resources and skills, to achieve their common mission / goal, but that is not limited to an alliance of profit enterprises. A virtual enterprise is therefore, a particular case of virtual organization."

"VO Breeding Environments (VBE) – represents "strategic" alliance of organizations (VBE members) and related supporting institutions (e.g. firms providing accounting, training, etc.), adhering to a base long-term cooperation agreement and adopting common operating principles and infrastructures, with the main goal of increasing both their chances and preparedness of collaboration in potential VOs".

This paper focuses on modeling trust to support understanding of rational trust concepts in member organizations of the VBE for the purpose of smoothening collaboration of those members in VOs. While addressing the need for supporting understanding the concepts of trust in organizations it is important to also consider what kind of actors shall be involved and for what objectives regarding their involvement. In our research we address these specific research aspects considering among other the three main trust objectives in organizations.

The first trust objective is related to the **creation of trust among member organizations** within the VBE. This objective aims at creating trust among organizations in a VBE to enhance the efficiency and success of both their cooperation within the network, as well as their potential collaboration while addressing a business opportunity in a short term goal oriented network, namely, VOs. Further to the achievement of individual organizations, the main aspects that influence the level of trust in a specific organization towards other organizations are mainly its past performance and good behavior in activities

within the VBE, as well as from its participation in short term opportunity based networks such as VOs. In addition, other aspects that may influence an organization's level of trust include its roles, reputations, membership commitment in the network, and so on.

The second trust objective is related to the **creation of trust of an organization to the leadership/administration** of the VBE. Trust of a member organization towards the consortium administration enhances the chance of the specific organization remaining loyal to the network, increases its willingness for active involvement in the network, and encourages the respective member organization to invite and bring other valuable organizations into the consortium. Among the main issues that influence the creation of trust in member organizations towards the consortium administration are found to be: successes in managing the consortium environments, a consortium's successes in external markets and recognitions achieved through consortium's marketing and branding, the transparency of the administration procedures and rules, the transparency and efficiency of procedures used for measuring the performance of member organizations, the frequency of and support for collaboration opportunities brokerage, and an equal opportunity for all member organizations to get involved in potential opportunities.

The third trust objective is related to the **creation of trust of the external stakeholders to the VBE**. A VBE must be trusted by its external stakeholders, including invited organizations and customers. On the one hand, invited organizations must be convinced that the network environment is trustworthy for their businesses and, in addition, that they will benefit more than they would if they were to work individually. On the other hand, customers that create business opportunities in the market (to which VBE can respond by creation of VOs) must recognize and trust the network in order to accept its proposed bid. Consumers (end users of results of the VBE) also need to trust the collaborative network in order to decide positively on purchasing or accepting the VBE's products and services that have been provided through short term consortiums in form of VOs.

2. Definition of terms and basic concepts

The concepts of trust are interpreted and perceived differently for various actors. Consequently, these differences affect the understandability of the base definitions and concepts of inter-organizational trust in research and practice. In this article we use the following definitions of base concepts of trust parameters for organizations.

Trust: Trust between two organizations, as it is applied in VBEs, is the objective-specific confidence of a trustor organization to a trustee organization based on the results of rational (fact-based) assessment of the trustee organization's level of trust.

Trust level*:* refers to the level of intensity of trust for a trustee organization in a trust relationship, based on an assessment of the values for a set of necessary trust criteria. Clearly enough, the criteria for assessment of organizations' level of trust vary and have a wide spectrum, depending on the specific purpose (e.g. the requirements, the perspective, and the objective of the establishment of trust). When the level of trust is assessed for a specific purpose - such as inviting a member into a VO - and the assessment is based on specific trust criteria for that specific purpose, the evaluated trust level results are referred to as the *specific trustworthiness* of that organization.

Trust actors*:* refer to the two parties involved in a specific trust relationship. The first party is the organization that needs to assess the trustworthiness of another, and is referred to as the trustor. The second party is the organization that needs to be trusted and which will thus have its level of trust assessed; and it is referred to as the trustee.

Trust relationship*:* a relationship is a state of connectedness between people or organizations, or a state involving mutual dealing between people or parties. Here, trust relationship refers to the state of connectedness between a trustor and a trustee whose intensity is characterized and based on the trust level.

Trust objective: is the purpose for which the establishment of a trust relationship among the involved organizations is required. Examples of trust objectives include the following: for inviting an organization to join a VO, for appointing or selecting an organization as the VO coordinator, for an organization to decide to join VBE, and so forth.

Trust perspective: represents the specific "point of view" of the trustor on the main aspects that must be considered when assessing the trustee's level of trust. The trust perspectives help the trustor organizations in deciding what information related to trustee organizations should be considered primarily, or secondarily, etc., and made available to them in order for them to create the required level of trust.

Trust requirements: represent the essentials (cardinals) that characterize and guide on how the respective trust perspective shall be realized. Thus, trust requirements are the fundamental cardinals that guide or suggest what must be met in order for the respective trust perspective to be realized. For instance, "financial stability" is an example requirement that must be met, to support establishing trust based on the economical perspective; similarly, "compliance with community standards" is a requirement for trust related to social perspective, and "stability in management" is a requirement for managerial perspective.

Trust criteria: represent the measurable trust elements that characterize each respective trust requirement. Therefore, the values of each organization's trust criteria

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

354

can be used to make a rational (fact-based) judgment on whether the respective trust requirement is met. Each trust criteria has its own related value structure that defines the acceptable structure for its data, such as the scalars, vectors, arrays, list of strings, and so on. Furthermore, such value structure also defines the metric to be used to scale the specified data. The only source of data for trust criteria is the respective trustee's organization. Therefore in each VBE, member organizations shall submit data related to their trust criteria, and keep them up-to-date. Data related to the trust criteria of organizations will be used in the VBE for different purposes related to trust management.

3. Classification of models of trust

Modeling of trust has attracted a number of initiatives from academicians which has led to development of many variants of trust models. Since the resulted models are built on different underlying concepts there is a need for developing systematic approach that can be applied to categorize, evaluate and improve these models in order to unify, standardize and apply them. In relation to collaborative networks, we categorize models of trust into **hard-models**, **soft-models and semi-soft-models** as further described below.

3.1 Hard-models of trust

These models of trust are designed to support the management of trust among organizations on basis of fact-based data, such as their performance data. This class of trust models have been developed and applied to support management of trust in some specific cases where reasoning on the achieved trust analysis results is necessary. In research addressing security of distributed systems, hard-models of trust support the management of trust among communicating systems. These models can detect and analyze trust based on data delivered through crypto-based mechanisms [Gulati & Singh, 2008].

Furthermore, in security studies of systems, hard-models of trust are applied to develop mechanisms that can be used to analyze trust applying data related to violations of security assumptions, security performances, vulnerability, etc. In our previous work on inter-organizational trust we have proposed hard-models of trust based on mathematical equations [Msanjila, & Afsarmanesh, 2008a]. Models are applied to formulate mechanisms for assessing the level of trust in organizations considering measurable criteria and a formal reasoning on results is supported.

Therefore, a number of different kinds of hard-models of trust are already developed for specific application cases. Hard-models do not consider the aspects of all stages of trust life cycle which is characterized with some soft aspects of trust as further

addressed in (b) below. *Thus there is a lack of conceptualized hard-models of trust that are comprehensive enough to adequately apply in any emerging objectives and can be customized to meet interests of any kind of organizations.* Although hard-models of trust provide a base or foundation for designing other models which consist of qualitative elements (soft-models) there is a need for looking into the possibility of integrating the two types of models.

3.2 Soft-models of trust

These models of trust are designed to support the management of trust among organizations on the basis of subjective data such as recommendations, reputation, opinions, etc. Soft-models of trust capture the trust relationships between organizations that are based on observable evidences about trustee's behavior, either through direct experience (witness reputation) or indirect experience (certified reputation). Hence soft-models of trust use social control mechanisms, namely, based on how actors socially recommend each other. Analysis approaches for soft-built trust include: probability measurements based on positive and negative opinions, logical operations to analyze trust transitivity, prediction analysis in relation to risks, etc. Existing models of trust for inter-personal interactions can be classified as soft-models [Gambetta, 1988]. While each type of models is able to provide a different focus on addressing trust issues, both types also come with some drawbacks. Hard-models of trust are difficult to apply in real life as they demand a complete set of data for all considered criteria. Soft-models of trust suffer from the lack of traceability and the problem of trust saturation leaving actors vulnerable to cheat attacks.

3.3 Semi-soft-models of trust

These models capture some aspects of both rational and subjective trust analyzes. Some attempts have been made by researchers to develop models which can capture a few aspects of both had-models and soft-models of trust, here referred to as *semi-soft-models* of trust. A causal model as inspired in the discipline of systems engineering supports analysis of causal influence among measurable factors (hard-model aspects) but allows some qualitative reasoning to be made on the nature of influences (soft-model aspects). For example, as shown in Figure 1 while factors "cash capital" and "capital" are both measured quantitatively with numbers the influence of cash capital on capital is qualitatively assumed as positive. Causal models as semi-soft-models of trust can also be transformed to hard-models of trust in form of mathematical equations. On the basis of assumptions as inspired by

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

355

the discipline of systems engineering the formulation of mathematical equations (hard-models of trust) can be achieved by applying causal models (semi-soft-models of trust). The equations are then applied in designing mechanisms for assessing the level of trust in an organization. For example, the equations for capital (CA) and financial acceptance (FA) is:

$$CA = CC + PC + MC \quad \text{and} \quad FA = \frac{SC}{RS}$$

Where CC represents cash capital, PC represents physical capita, MC represents material capital, SC represents standards complied, and RS represents required standards.

Furthermore, semi-soft models can also be transformed to fully soft models by assigning qualitative values into measurable parameters. Such values can be inform of low, medium, high or any other value of similar nature of qualitative.

4. Models of trust in CN

Research on trust is characterized by a substantial diversity in disciplinary background, methodologies, models, and definitions. These differences result mainly from variations of actors' perceptions of what it means to trust. By the same token as the differences in interpretation of trust, diversity also exists among the current hard models of trust in organizations developed by these same researchers. Several examples of existing trust models are discussed in this section, and although they are originated and applied in different environments, each one presents some aspects that are related to the VBEs.

4.1 An integrated model of trust in e-commerce

Electronic commerce, commonly known as *e-commerce*, refers to buying and selling of products or services over electronic systems such as the Internet and other computer networks.
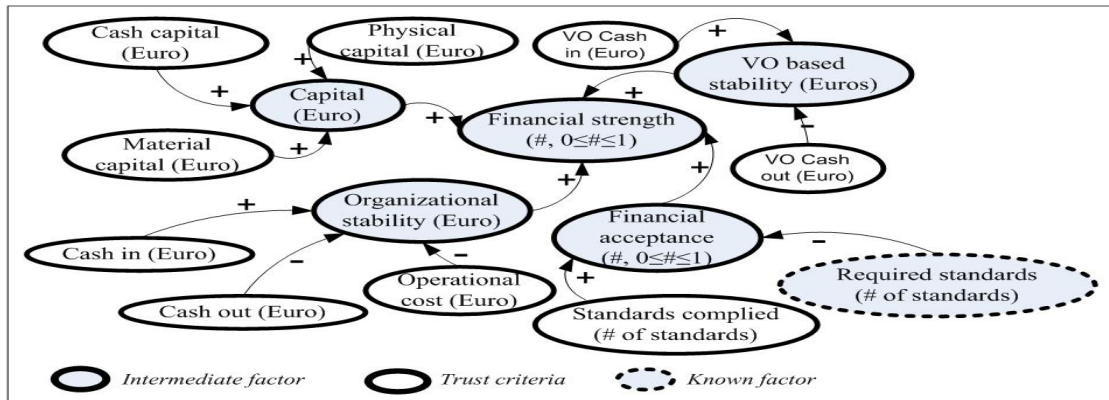

Fig 1: Semi-soft-model of trust for the organizational economical perspective

A wide variety of commerce is conducted in this way, benefiting on innovations in a number of business aspects including: electronic money transfer, supply chain management, internet marketing, electronic data interchange, inventory management systems, automated data collection systems, etc. Modern e-commerce uses the World Wide Web, at least at some point in the transaction's lifecycle, although it can encompass a wider range of technologies. A large percentage of e-commerce is conducted entirely electronically for virtual (non-physical) items, such as access to premium content on a website, issuing electronic tickets for flights, buying soft version of software, etc. However, other e-commerce transactions may also involve the transportation of physical items to buyer in some way once the ordering and payment are accomplished electronically.

Past research has pointed out a number of challenges that need to be addressed in order to

facilitate the full realization of e-commerce. Some few challenges to exemplify here are: authentication of users with their specific and unique identification and role, assurance of the privacy of involved actors, support for online negotiation, management of online payments, personalization of e-commerce services, establishment of suitable infrastructures, creation of support software, etc. [Keen, 1999]. In addition to these challenges, a key challenge, related our research, is the establishment of trust among actors involved in the e-commerce transactions. In fact transactions taking place in e-commerce are similar to the business processes conducted and/or supported in VBEs, in the sense that they are both handled virtually and in distributed environments. Thus the concepts of trust among actors involved in e-commerce and related trust models can be fundamental input to understanding and modeling inter-organizational trust. To support the understanding of trust among actors in e-commerce

and its related transactions, Kini and Choobineh [1998] developed a theory that provides a strong theoretical foundation for a set of factors influencing trust related behaviour. The model is based on fundamental assumptions that trust in an online system is a function of the four dimensions (Figure 2): (1) Characteristics of the person making the e-commerce transaction; (2) The online system itself that supports the required transactions; (3) The task for which the system is being used; (4) Trust information and its source environment. As shown in Figure 2, all four dimensions influence the creation of trust between the partners involved in the e-commerce transactions.

In their study, Kini and Choobineh [1998] proposed that it is the **personal** characteristics of an individual or the behavior of the managerial team of an organization which determine his/her readiness to trust. Other researchers who have studied individuals'

trusting behavior also contend that the readiness to trust is shaped by specific developmental and social-contextual factors [Lee & Turban, 2001]. In this model, this readiness characteristic is called *Tendency To Trust* (TTT). This research demonstrated that people with a high TTT are more willing to trust others when confronted with new situations. To further understand the TTT in relation to specific transactions, it is important to study the kinds of **task** that necessitate trust, and to focus on means of fostering and developing trust in these tasks in order to ensure that *e- commerce systems* can be developed for a wide range of applications. The sensitivity of a **task** being executed using the e-commerce technology might make the creation of trust among e-commerce actors difficult. For example, whether the task needs to be accomplished completely online or some physical processes are needed.
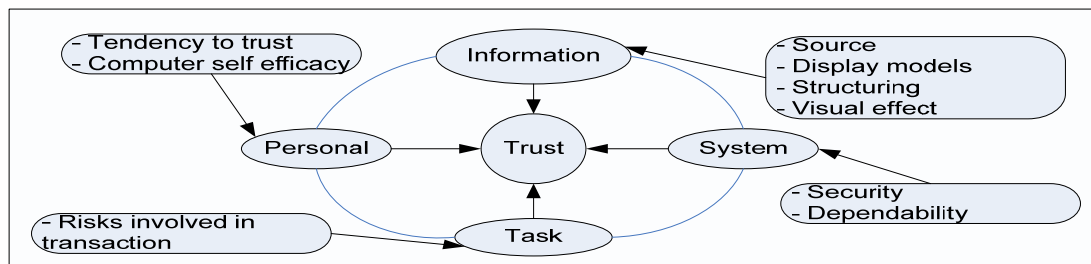

Fig. 2: An integrated model of trust for E-commerce application

Also, the gains expected by actors and the risks that can emerge by handling the task using e-commerce technologies, as compared to other approaches such as physical transactions, might influence the decision of an e-commerce actor to trust others. The characteristics of the **system** with which the user interacts play a critical role in the development and preservation of trust between partners in e-commerce-based transactions. Several studies have shown that security is a main factor in the success of online businesses [Msanjila & Afsarmanesh, 2007c]. Other factors influencing creation of users' trust in the system are their perceptions of dependability and reliability of the system itself.

The **information** which needs to be exchanged to support e-commerce transactions has an important role in realizing the required trust among e-commerce actors. The content of information which needs to be exchanged among e-commerce actors must be as accurate, valid, up-to-date and complete as possible. Furthermore, the reputation of the environment where the information is collected *(source's environment)* and usability of environment where the e-commerce actors access the information *(online system interfaces)* might influence the decision of actors to trust others. For example, the usability of the system

influences the willingness of customers to in detail read the online advertisements of products and services and thus decide on which provider to trust. The environment presented by the system – user interfaces - should be correctly perceived and understood by users in relation to the presentation and structuring of the information. Therefore, visualization and display models are critical issues that must be taken into account in order for the information to be successfully exchanged among e-commerce actors. The effects of system's user interfaces should be studied to guide the design and implementation of suitable interfaces. In particular, it is important to identify whether different presentation modes, such as websites based on frames, multimedia, dynamic/static website, and so on, affect the creation of trust among e-commerce actors using online systems.

The external environments –surrounding environments such as the competitor markets – might also influence the creation of trust between actors by providing them with complementing or contrasting information. It also contributes to the overall perception of the reliability, security, privacy, dependability, etc. of a system supporting the e-commerce transactions. It is important to understand whether trust in a system can be manipulated by

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

357

providing information on possible external impacts relating to relevant aspects of the system.

Relevance to our research: *As described earlier, the virtual and distributed nature of e-commerce transactions is similar in the way business processes are handled and supported in VBEs. In relation to the work addressed in this article, the approach for characterization of elements that are included in the e-commerce trust model, as exemplified here, is relevant and complementary. Specifically, concepts presented in this model are applied in our work to analyze a number of trust related aspects among organizations in VBEs, as addressed below:*

- *Trust related information to be exchanged among organizations*: We have applied the concepts presented by this model to analyze the content of information that is needed to be provided to a trustor organization in order to trust a trustee organization. Applying the knowledge gained through learning this model we have characterized the content of organizational data related to trust on the basis of five aspects, namely: *"why", "what", "when", "how" and "who"* as further addressed in [Msanjila & Afsarmanesh, 2008a]. We have also applied the concepts presented by this model to analyze the need for information to be accurate, valid, up-to-date and complete for the purpose of enhancing the effectiveness of the process for creating trust.

- *Technological aspects supporting organizational collaboration*: We have considered the concepts presented by this model to analyze the influence of technology (related to technological perspective such as information systems, on the process of creating trust among organizations. The success of creation of trust between collaborating organizations is influenced by a number of various aspects related to the technological perspective. Information and communication systems that are applied by an organization or by the VBE to facilitate the collaboration among organizations can influence the decisions made by those partners about trusting each other. System related aspects, such as security, privacy, reliability, etc., unless handled properly by the VBE and by organizations can negatively influence decisions made by organizations to provide their trust related data to the VBE administrator or the trustor organization. So, there will be a lack of trust related data and as a result organizations will face difficulty in trusting each other.

4.2 A trust model for inter-organizational network effectiveness

This trust model has been proposed as a means to support and provide guidelines, and act as a driver, to organizations that are participating in cooperation/collaboration networks [Ahuja, 2000]. The aim of this model is to increase the chance of an organization for achieving their common or compatible goals, and thus improving the effectiveness of their VBE. The focus of this model is on how inter-organizational networks can benefit from and

influence strategic resource acquisition (Figure 3). This proposed model addresses factors relating to the structural and relational dimensions of social capital built between organizations in a VBE. On the basis of this model, organizations can analyze the effectiveness of their network in relation to the following:

- *How collaboration between organizations influences the potential for achieving common goals.*
- *How achievements of common goals improve the network's effectiveness.*
- *How trust affects organizations' collaboration especially in relation to sharing and exchanging information, resources, etc.*
- *What are the relations between network performance and individual organization's performance?*

A VBE can ultimately enhance the performance of its individual organizations by supporting different forms of collaboration which best fit the needed response to acquired opportunities. For example, an organization's innovative capabilities are positively impacted by both direct and indirect forms of well-established communication with other organizations. This communication enables knowledge sharing between the cooperating or collaborating organizations and the opportunity for them to provide each other with complementary skills [Msanjila & Afsarmanesh, 2007a]. The different forms of collaboration and their transactions reflect organization configurations in collaborative networks [Ahuja, 2000].

Researchers have explored the impact of collaborative network configurations, focusing on the number of involved organizations and the hierarchies in making decisions, on outcomes and effectiveness of their collaborations [Human & Provan 1997; Gloor, et al., 2008]. The results indicated that the level and range of performances achieved by organizations in networks might be influenced by the number of involved organizations and the manner of their involvement. For example, a network with large number of member organizations has high chance of internally constituting a large set of competencies and thus is able to quickly and efficiently respond to emerging business opportunities. The results also indicated that in a flat network in which decisions are collaboratively made (decentralized network) there is high chance of making acceptable and effective decisions by all involved organizations. Although communication between organizations alone can represent a significant level of sharing and exchanging resources, this does not guarantee the actual transfer or exchange of strategic resources in the network. There are three fundamental barriers that encumber the transfer of strategic resources among organizations in the network [Szulanski, 1995; Hurmelinna-Laukkanen & Blomqvist, 2007]:

- the receiver's lack of absorptive capacity;
- causal ambiguity within the interactions;

✦ weak relationship between the source and the receiver. It was observed that trust helps to overcome all three of these barriers and that it also encourages an important condition for the exchange of resources to occur, namely the *motivation* [Ahuja, 2000]. Without trust, organizations will be reluctant to share resources due to the fear of possible risks that might arise, such as the opportunism from other collaborating organizations. This model implies that the level of trust affects the number and level of resources that can

be exchanged. It also implies that the level of trust is related to the difference between the number of resources that organizations are willing to transfer and the amount that they are actually able to transfer. Consequently, the effectiveness of the collaborative network is dependent on the level of trust from its member organizations. This indicates that the amount of resources acquired through networking is related to the balance of trust levels between organizations.
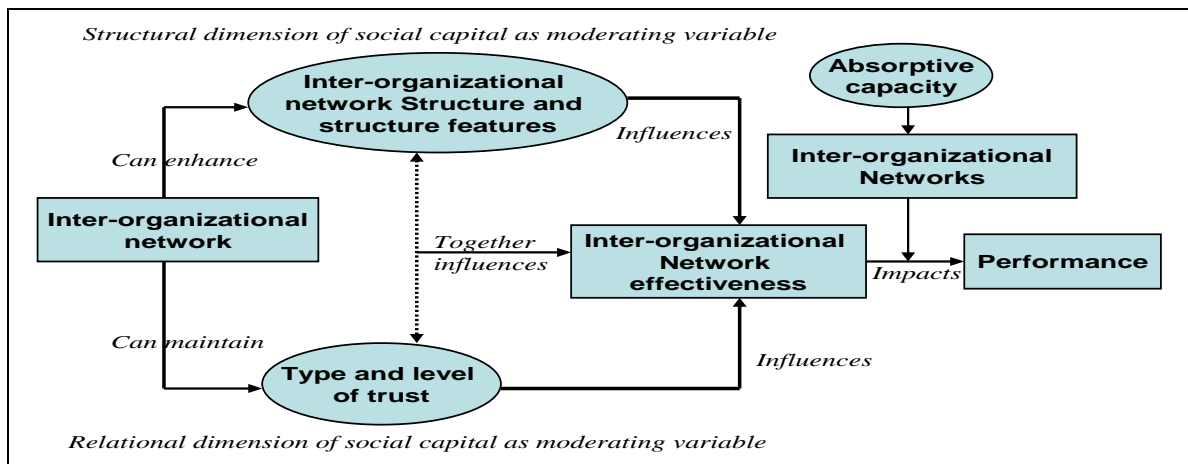

Fig. 3: Conceptual model for trust and network effectiveness

Relevance to our research: *The main input data to the assessment of the trust level of an organization, as characterized in our approach, is its performance data. The performance of the VBE as a whole and its configured VOs, represent the collective performance of all involved organizations. Different aspects presented in this model which influences the performance of both – the network and the member organizations – such as absorptive capacity of organizations, causal ambiguities within interactions, willingness to exchange and share resources, etc. - are of importance for our model of trust.*

We have considered the concepts presented by this model to better understand how VOs need to be configured, and especially related to constituent partners that are selected from the VBEs, to enhance the chance of optimizing the performance of both individual organizations as well as the VO itself, which in turn will enhance their trust level. As such, a VO should be configured constituting the set of most trustworthy partners in the VBEs for each specific trust objective. As presented by this model, strong trust among organizations has positive impact on the effectiveness of their collaboration and their individual organization's performances, which in turn shows that there is a causal feedback between trust in an organization and its performance in collaboration.

4.3 FIRE: Trust model for open communities

An open community is a group of people that primarily interact via communication media, such as

letters, telephone, email or Internet rather than face to face; for social, professional, educational or other purposes. If the mechanism applied to support the interactions among actors is a computer network, such as the Internet, then the community is called *an online community*. The ability to interact with like-minded individuals instantaneously from anywhere on the globe has considerable benefits, such as possibility to acquire knowledge from any place in the world. But these open communities have bred some fear and criticism mostly due to their virtual nature. It has been stated that these communities can serve as dangerous networking or hunting grounds for online criminals, such as identity thieves and stalkers, with children particularly at risk [Sharratt & Usoro, 2003]. Of particular interest to our research is how the trust of the involved actors is assessed, analyzed and assured. One source of information needed to analyze and understand trust of actors in open online communities is the reputation of each actor.

FIRE - an acronym that is created from first two letters of the word '**fi**des', which is Latin for 'trust', and the first two letters of the word '**re**putation' - is a reputation-based model of trust that has been proposed as a means to support a common understanding of trust between actors in open communities [Huynh, et al., 2004]. It provides an explicit representation of uncertainties, yet is only used to add weight to

different nodes (actors) during the complete trust integration (creation) phase. It also employs a very simple approach for the aggregation of reputation information. The modelers enhance the performance of their model by separating different types of trust and reputation, but they do not reach the level represented in the trust model. The FIRE trust model integrates four types of trust and reputation aspects:

- *Interaction trust* resulting from past experience of direct interactions,
- *Role-based trust* defined by various role-based relationships between the actors,
- *Witness reputation* built from reports of witnesses about an actor's behaviour,
- *Certified reputation* built from third-party references provided by the actor itself.

The inter-relation between trust and reputation is not clear in this model and in particular, how the data on reputation is manipulated while analyzing trust of actors. Therefore, the function of evaluating trust may fail to account variations of reputation when the reliability of the actor's behaviour changes with time.

Relevance to our research: *Although the trust model for open communities addresses the trustworthiness of individuals, the nature of the environment in which this model is applied have some similar characteristics to those of the VBE – mainly, its virtual collaboration nature.*

Therefore different aspects related to analyzing trust of individuals in open communities, who can virtually interact without physically knowing each other, are relevant input for studying trust among member organizations of VBEs.

4.4 Taxonomy-based trust model for supporting an understanding of multi-agent systems

In recent years there has been a significant growth in the field of multi-agent systems in both research and practice. As applied to collaborative networks, an agent represents an organization rather than an individual or a system. One challenging issue in this field relates to the provision of support, which is necessary to facilitate cooperation between different agents and is fundamentally related to a computation of their reputations. Several researchers addressing MAS have discussed this challenge and suggested a number of reputation models that appear in the literature offering solutions to this problem. However, most of these solutions introduced specific concepts, terminologies and specific ways to represent reputation models and manipulation mechanisms [Korba & Song, 2003]. Consequently, it is difficult to achieve a "hypothetical understanding" of reputation evaluation among agents using different reputation systems [Pinyol et al., 2007].
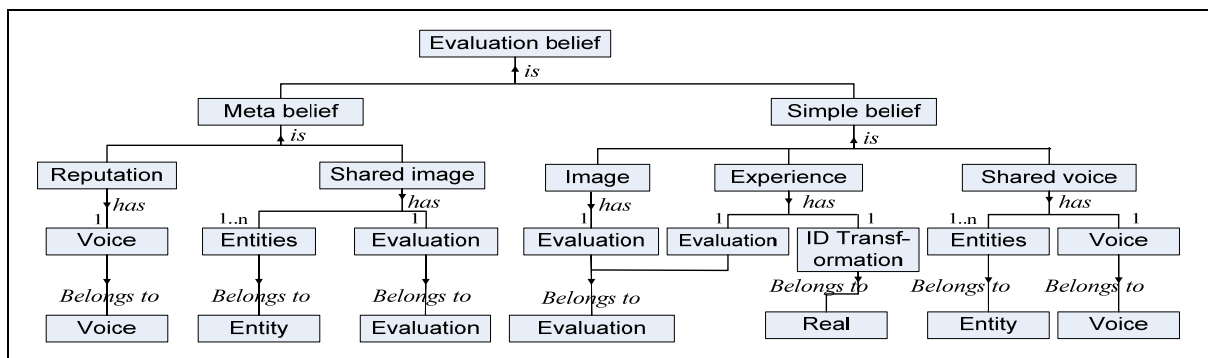

Fig. 4: The taxonomy, membership relations, and components of evaluation of belief

To address this problem Pinyol et al., [2007] have proposed a trust model based on ontology (taxonomy) that aims to support agents to achieve the required level of common understanding of trust and, in particular, the mechanism they use for assessing reputations. A number of characteristics are considered for this purpose and included in the ontology, as illustrated in Figure 4. The key elements which the model examines are an agent's belief and its social evaluation, which are affected by a number of other subordinate elements, as shown in Figure 4. The model proposes a fundamental solution that can be implemented for exchanging the results of social

evaluations of agents using different reputation models within the same multi-agent system paradigm.

Relevance to our research: *Supporting the member organizations of the VBE within a network in achieving common understanding on concepts related to their trust, is as important as the creation of the trust itself. The taxonomy based model is developed to support agents with achieving common semantics on related reputation based systems. This model and its constituent concepts are consider in our research to understand how the concepts of inter-organizational trust need to be classified, and later on to be presented to organizations for the purpose of enhancing their understanding of trust concepts as applied in the VBE environment.*

4.5 Federation for Identity and Cross-Credentialing Systems (FiXs)

This trust model is developed by FiXs [www.fixs.org]. The Federation for Identity and Cross-Credentialing Systems (FiXs) is a coalition of commercial companies, government contractors, and non-profit organizations whose mission is to establish and maintain a worldwide, interoperable identity and cross-credentialing network. This network is built on enforced security, privacy, trust, standard operating rules, policies, and technical standards. The FiXs network verifies and authenticates the identity of personnel seeking to enter the U.S. military installations and other government-controlled areas, as well as the commercial sites tied to the network. FiXs provides a trusted mechanism for federated identity infrastructure within and between public and private sector organizations with accuracy through the application of a so-called "Federated Trust Model". The network services supported by the trusted mechanism can be accessed worldwide, in remote or fixed environments, wired or wireless, and in real-time. A key component to the network integrity is its strong credential authentication and revocation processes, as governed by the FiXs operating rules.

The Federated Trust Model defines an underlying foundation that guides the common operating rules and legal procedures of the Federation of Identity and Cross-Credential Systems. It enables all participants and advisors to keep their existing security systems and policies intact, while strengthening their credentialing processes, in order to achieve balanced levels of trust within a shared infrastructure. The model is based on the concepts of community trust and brokered trust (Figure 5) [FiXs, www.fixs.org].

Relevance to our research: *The trusted mechanism that supports organizations' access to network services, and the trust model which defines the common operating rules and legal procedures for collaboration, are the fundamental concepts applied to the establishment of trust among interacting actors who use the federated identity infrastructure. Member organizations of the VBE are typically in geographically dispersed locations. Therefore, the concept of federation introduced in this trust model helped us to understand and learn about how the analysis of trust among organizations can be performed when considering the need for interoperability among their systems. As such, the interoperability aspect of organizations is analyzed, considering the level by which the organizations' information systems meet the following elements of the VBE: formulated policies, operating rules, security guidelines, specified architectures, etc. Furthermore, these concepts are applied in our work for better understanding of the need for sharing and exchanging information and knowledge between member organizations of the VBE and the influence of the results of these processes on inter-organizational trust relationships.*
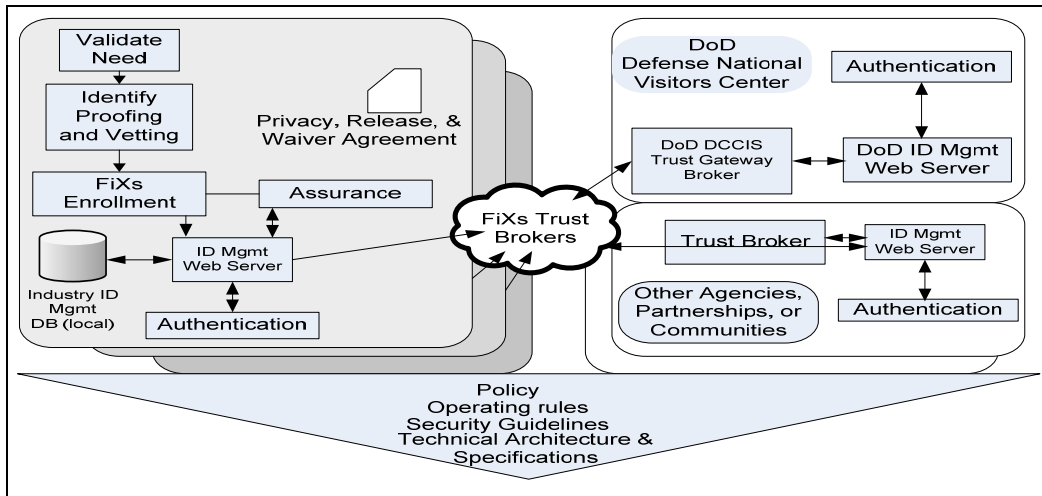

Fig. 5: Trust model for the Federation of Identity and Cross-Credential Systems

4.6 Direct: A trust model for the process of creating VOs

This model is based on reputation and is applied in the process of creation of VOs [Avila-Rosas & Luck, 2005]. As such, the potential partner organizations will decide to accept or reject an invitation for the short term consortium such as VOs on the basis of each other's reputations. The model also eases the process of assessing and selecting the most suitable set of network member organizations for a short term consortium. The reputations are assessed on the basis of personal and mediated experiences by applying certain reputation systems. Information on reputations is based on what one party has said about another

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

361

party over time, and the history of the interactions of these parties with others [Lucas, 2005].

Reputation systems have been addressed by a number of research and development projects. These systems are used in various applications, among others, in e-commerce to assess the trust of buyers/sellers, and in collaborative environments to assess trust of potential partners. As implemented in various systems, *reputation* is a function of the cumulative positive and non-positive ratings/opinions for an actor over the recent periods (weeks, months, years) related to how it is known and perceived by others [Resnick & Zeckhauser 2000]. Reputation systems are applied to analyze the collected reputation data and provide results about the subjective trustworthiness of actors for a particular purpose.

Despite the obvious usefulness of reputation and related concepts for collaboration, such as in supporting exchanging and transferring knowledge between organizations [Lucas, 2005], there are still some existing conceptual gaps in the current developed and applied models. Resnick and Zeckhauser [Resnick & Zeckhauser, 2000] have pointed out the so-called "*Pollyanna*" effect in their study of a larger set of reputation systems. In relation to this effect, it has been observed that there is disproportionately positive feedbacks from users and rare negative feedbacks which in turn makes the results from the analysis in most cases biased and do not represent the actual true picture.

Relevance to our research: *One fundamental strategic goal of the VBE is to support their member organizations to rapidly and efficiently configure VOs in response to brokered opportunities. A fundamental indicator for potential partners (organizations) of the VO is their trust level. As proposed in our research the main input data to the assessment of organizations' trust level is a set of their measurable fact-based data e.g. in relation to their performance. However, in some cases the performance data of organizations might not be up-to-date or some measurable data might be missing / incomplete. In such case, the organizations' reputation can be applied instead to indicate their actual trustworthiness subjectively. Thus our research has benefited from the presented concepts in this model as a fundamental input to understanding the process of complementing the rational analysis of trust in potential partners of VO with subjective trust analysis, if it is needed.*

5. Modeling of trust relationships

In order to accurately model trust relationships between organizations and to represent their related components, we have chosen to base the definition of our models of trust on the following three formalisms.

- *Ontology-based models* of trust relationships between organizations: to support organizations achieve and maintain common understanding about the fundamental concepts of inter-organizational trust.
- *Object-based models* of trust relationships between organizations: to address cardinalities of relationships between trust elements, which are used for the implementation of functionalities of the Trust Management (TrustMan) system.
- *Record-based models* of trust relationships between organizations: to provide a rough relational database schema, and thus applied to the design of the database for organization's trust related data.

Although the models resulted by applying these three modeling formalisms constitute some similar parameters, each of these three models of trust relationship between organizations is developed to cover certain specific aspects and support our research in achieving different purposes related to development of organizational trust management system.

A priori to modeling trust relationships between organizations, we have to identify and classify trust aspects and factors that need to be included in the models. A challenge is that of ensuring that the model incorporates and covers all basic and advanced concepts as perceived in the targeted domain through requirement analysis with the users of the environment. As such, each designed conceptual modeling is correct and complete, while clearly not unique for representing the addressed concepts, entities, characteristics and their inter-relationships.

5.1 Main trust parameters for modeling trust relationships between organizations

Trust parameters that need to be included in the conceptual model of trust relationship between organizations have been divided into five main groups, namely: the *trust actors, time, level of trust, trust relationship, and trust elements*. Below we provide formalized descriptions for each parameter in order to enhance the understanding of the models of trust relationships among organizations.

i) *Trust actors: Trustor and Trustee:* The two parties in the trust relationship, namely the trustor organization and the trustee organization, are important when defining, modeling, and creating trust in VBEs. In general, a variety of factors might be required by different trustor organizations for assessing the level of trust in the same trustee organizations, even if the trustors have the same "objective" in establishing trust relationships. Therefore, it is important that both the trustor organization and trustee organization are distinctly represented in the model of their trust relationship.

ii) *Time: Past, Present and Future:* A trust relationship (and its intensity) between two organizations is an

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

362

issue of time, which may differ today or tomorrow from how it was yesterday. In other words, an organization's level of trust is not static and may vary depending on changes in the set of trust criteria, the values of the trust criteria, involved trustor organizations, specific ratings of trust level, and so on. All of these factors, which have the potential of influencing changes in an organization's level of trust, are time sensitive. Thus time is an important factor, and must be properly addressed when modeling trust relationships between organizations in VBEs.

iii) *Trust level:* Trust level refers to the intensity of the level of trust for a trustee organization in a trust relationship, on the basis of an assessment of the values for a set of necessary trust criteria. Therefore, the trustee's level of trust is an important aspect to consider for each trust relationship between two actors. Accordingly, this aspect is considered in the model of trust relationship between organizations.

iv) *Trust relationship:* Generally, a relationship is a state of connectedness between people or organizations, or is a state involving a mutual association between people or parties. Trust relationship here refers to the state of connectedness

between a trustor and a trustee, the intensity of which is characterized and based on the level of trust. In our modeling approach, trust relationship is the primary parameter of the trust model.

v) *Trust elements:* One important aspect of characterizing trust in VBEs is the identification of trust elements for various organizations. We have found that trust elements considered for organizations are not at the same level of abstraction and/or measurability. Through requirement analysis with users we have identified a wide range of trust elements classified in trust perspective, trust requirements, and trust criteria as visualized in Figure 6. The identified trust elements are hierarchically-related, from abstract (non measurable) ones which represent the root and other high level nodes, to the measurable ones which represent the lowest leaf nodes in the hierarchy. Together these elements characterize the trust and trust relationships for organizations and their classifications represent the fundamental concept of inter-organizational trust, and in particular related to the assessment of trust level of organizations. Thus models of trust relationship between organizations must also capture and include all these aspects.
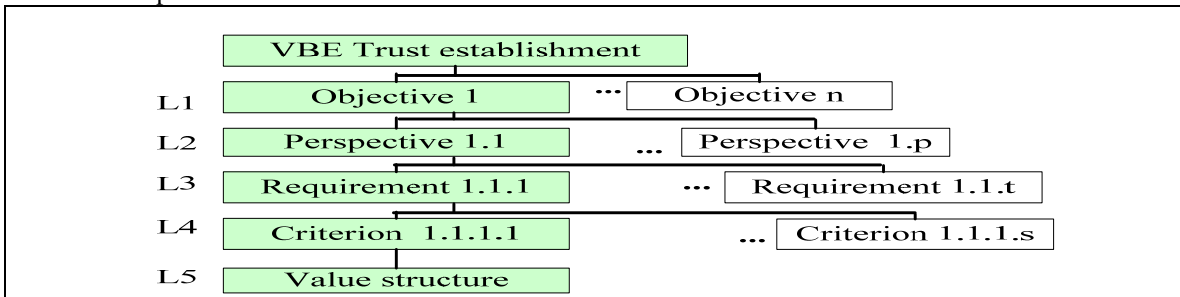

Fig 6: General view of hierarchy of trust elements

5.2 Object-based conceptual modeling formalism

In recent years, object-oriented modeling (OOM) has become the de-facto standard in early phases of software development in research environments. The current state-of-the-art for conceptual modeling is dominated by Unified Modeling Language (UML) which has been initiated and further stimulated by industry [Maciaszek, 2007]. With UML, Modeling can develop three kinds of models, namely the *static models, structural models, and transitional models*. In some cases the concepts represented in static models and structural models are combined to produce a more comprehensive design model. OOM constitutes the following seven modeling constructs:

- *Objects:* Entities that have state and attributes, and they provide services when initiated, instantiated and executed.
- *Classes:* Provide a way to categorize objects with similar attributes or services. Classes form an abstraction hierarchy through 'is_a' relationships.
- *Attributes:* These are used to represent an object's state. Modelers use attributes as a means to specify the type, visibility and modifiability of each function and procedure in the class.
- *Relationships:* Define how an object is related to another. Relationships can be classified as '*is_a*' classification relations, '*part_of*' relationships, and as having '*associations*' between classes.
- *Methods (functions and procedures):* These are the operations that all objects in a class can perform in

IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

363

order to provide the targeted output of the object when called on to do so by other objects.

- *Message Passing:* Provide a means for objects to invoke services that are provided by other objects.
- *Use Cases/Scenarios:* Provides a description on the sequences of messages exchanged between objects in order to facilitate the execution of a service.

The main aim of developing the model of a trust relationship between organizations, by applying object-based formalism, is to represent applied trust elements as objects that provide users with proper

ways of studying cardinality of a relationship between objects modeled to represent those elements. For example, defining the cardinality of the relationship between an object which is representing a trust criterion and another object which representing a trust perspective. Figure 7 shows an objective-based model of trust relationship between organizations. In Figure 7, TR represents the trust relationships, TRO represents the trustor organization and TRE represents the trustee organization.
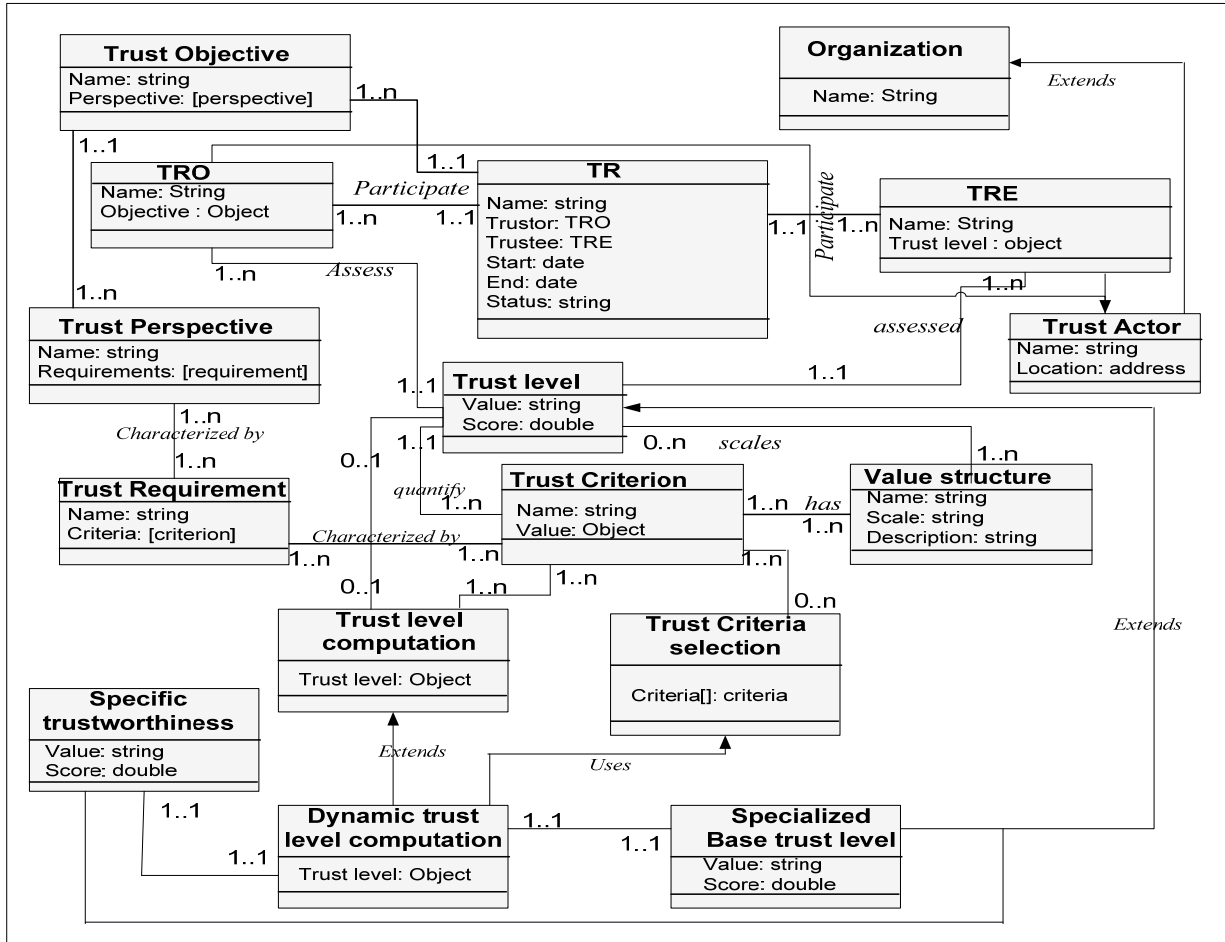

Fig. 7: Object-based model of trust relationship among member organizations

Understanding of relations among trust elements and the possibility to model these elements as objects, capturing the cardinality of the relationships among the objects, assist the developers in the process of implementing organizational trust management systems. The modules developed for supporting the computation of trust level of organizations, using the TrustMan system, are implemented as objects in Java programming language. Therefore, the object-oriented model of the trust relationships between organizations is used to guide developers with the implementation of

functionalities of the TrustMan system. The modules developed on the basis of this object-oriented model are also applied to classify the functionalities, on the basis of cardinalities of relationships among their implemented classes, into sets of integrated services.

5.3 Record-based conceptual modeling formalism

This formalism can be used to model trust relationships between organizations as records as inspired in the approaches for relational data

modeling. In this modeling formalisms, a trust relationship (TR) is modeled as a record constituting five attributes, namely: trustor organization (TRO), trustee organization (TRE), trust level of the trustee organization (TL), start date and status (equation (i)). The *status* indicates whether the TR is past, present or planned for future

$$TR = [TRO, TRE, TL, start\_date, status] \ldots\ldots\ldots(i)$$

Trust level of the trustee (TL) is also modeled as a record constituting three attributes, namely: the trust perspective preferred by the trustor organization (perspective), the trust requirements for each preferred trust perspective, and trust criteria for each trust requirements (equation (ii)).

$$TL = [Perspective, (requirements, (criteria))] \ldots(ii)$$

Furthermore, the trust criterion is modeled as a record of its value structure and value metrics (equation (iii)).

$$Criteria = [value\_structure, value\_metric] \ldots\ldots(iii)$$

The three equations (i to iii) together make the set of records constituting the record-based trust model for a single trustor organization to single trustee organization in a single trust relationship. If the respective trustor organization has multiple trust relationships with the same trustee organization, the attributes TL, start-date and status of the TR record (equation (i)) become repeating attributes. Repeating attributes are closed by parentheses and separated by commas. The representation of repeating attributes takes into account the fact that, although the actors are the same, it is possible that at different times there may be a different level of trust for each trust relationship between trustor organization and trustee organization. While records for TL and criteria remain the same, the TR record changes as shown in (iv).

$$TR = [TRO, TRE, (TL, start\_date, status)] \ldots\ldots\ldots(iv)$$

Furthermore, it is possible for a trustor organization to have many trust relationships with different trustee organizations (equation v).

$$TR = [TRO, (TRE, TL, start\_date, status)] \ldots\ldots\ldots(v),$$

A single trustee organization can also have at different times many trust relationships with different trustor organizations (equation vi). Moreover, these TR can have dissimilar intensity due to different levels of trust in the participating actors.

$$TR = [TRO, (TRE, (TL, start\_date, status))] \ldots\ldots\ldots\ldots(vi)$$

When the trustee organization has multiple trust relationships with different trustor organizations, the inverse of the records in equations (v) and (vi) apply as shown in equations (vii) and (viii).

$$TR = [TRE, (TRO, TL, start\_date, status)] \ldots\ldots\ldots(vii),$$

$$TR = [TRE, (TRO, (TL, start\_date, status))] \ldots\ldots\ldots(viii)$$

A formalized record-based representation of trust relationships between actors when a trustor organization is simultaneously a trustee organization and probably with relation to different trustee organizations and trustor organizations respectively needs to be modeled. For this case, the following *record-based model* of trust relationship between organizations is developed, as presented in a diagrammatic form in Figure 8. Figure 8 shows four nodes N1 to N4, and their trust related relationships, in which they may act as either a trustor or a trustee. In Figure 8 it is shown that the trustor TRO-1 has two trust relationships, one with the trustee TRE-2 and the other with the trustee TRE-3. However, the trustee TRE-2 is also the trustor as TRO-2 and it has two different trust relationships with the trustee TRE-4.
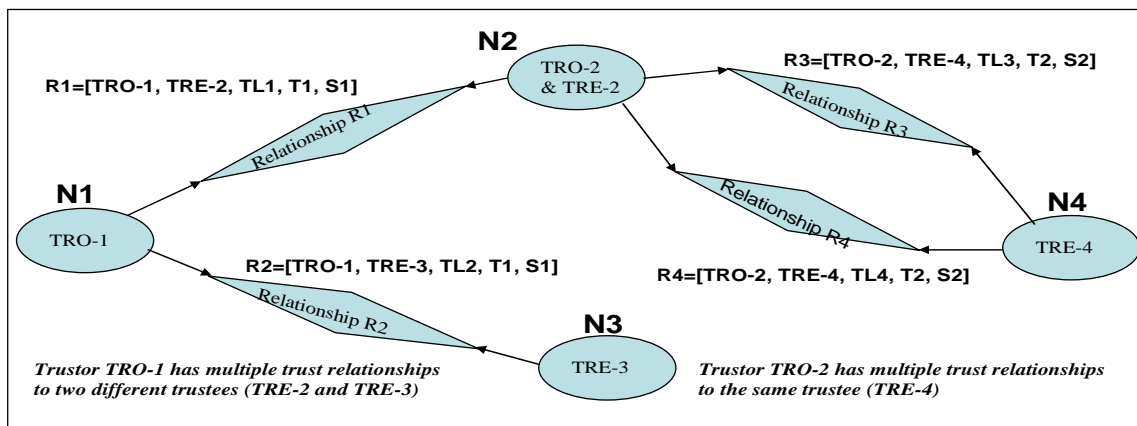

Fig. 8: Relationship-based model of multiple participations among organizations

One of the most challenging and central tasks in managing the trust between organizations is managing the data that is required to support the assessment of the organizations' level of trust. A traditional approach for

managing structured data is through maintaining a database. The main objective of data modeling in databases is to provide a data structure that adequately represents the real world and that can be processed efficiently by database management systems. Developing services supporting the management of data is an important part of the processes for managing inter-organizational trust. As a result, trust related data must also be correctly modeling and structured using some systems in order to enhance the effectiveness of its exploitation. Most existing databases and database management systems follow a relational approach. In order to enhance the interoperability and sharing of data that is managed by the TrustMan system with the existing/legacy databases, the database that we developed also adopted the relational approach. Therefore, in our design and implementation of the system for managing trust related data for organizations, we have used the record-based models of trust relationship between organizations addressed above to define relational database schemas detailing the required records and respective attributes.

Namely, based on the classification of trust elements as shown in Figure 6, we have designed three different schemas: *schema for general data related to trust elements, schema for general organizational data, and schema for trust related data of organizations*.

a. *General information related to trust elements* - This information constitutes a list and a set of descriptions of trust elements, namely of different trust perspectives, trust requirements, and trust criteria.

b. *General information about organizations* - This refers to the information that is necessary to accurately describe each physical or virtual organization. For physical organizations, this information may constitute the name, legal registration details, address, and so on. For virtual organizations, this information may constitute,

among others, the details of the coordinator of the VO, launching and dissolving dates, involved partners, and the customers.

c. *Specific trust related data for organizations* - This information constitutes the values of trust criteria for each organization. This information represents primarily the organization's performance data, expressed in terms of different trust criteria, and is used as the main input data for the services that assess the level of trust in each organization.

5.4 Ontology-based modeling formalism

In information sciences and engineering, ontology refers to 'an explicit specification of a conceptualization', 'a theory or a system of concepts/vocabulary used as building blocks for information processing systems', and 'a representation of semantics of terms and their inter-relationships'. A VBE environment is characterized by its dynamic characteristics, such as its environmental features, objectives, member organizations, etc. New ontologies for VBEs will continuously emerge and existing ones will evolve. Development of a trust related ontology will also undergo the same life cycle processes [Afsarmanesh & Ermilova, 2007]. The effectiveness of an assessment of level of trust and the acceptability of its results is greatly influenced by the common understanding of trust between its involved parties, including trustor organizations, trustee organizations, administrator organization of the VBE, and other stakeholder organizations. One approach for supporting establishment of such an understanding of trust is by providing these parties with an ontology describing the concepts and terms used for the various elements, features, principles, mechanisms and software tools [Afsarmanesh & Ermilova, 2007].
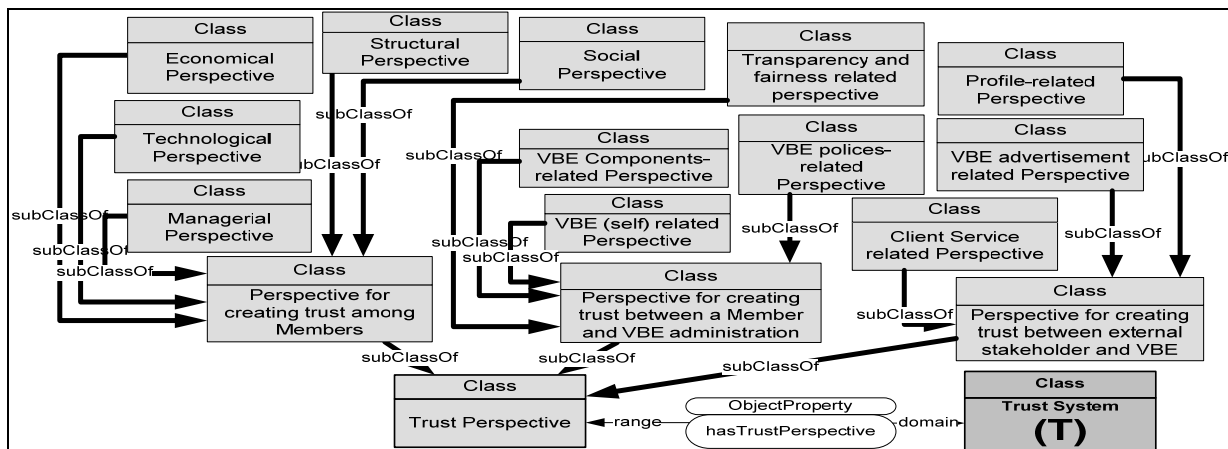

Fig. 9: Ontology-based model of trust relationship between organizations

For the specific purpose of supporting such common understandings on trust, we have developed an ontology-based model of trust relationship between organizations classifying the taxonomical relations between trust elements (Figure 9). This ontology is described for environment of the VBE and included within the *Ontology Discovery and Management System* (ODMS) developed with the ECOLEAD project [Afsarmanesh et al. 2008]. Concepts related to the level of trust in organizations, inter-organizational trust relationships, different trust elements, and so on must also be understood well by all of the actors within a VBE. Therefore, the ontology-based models for trust relationships between organizations are also applied to the implementation of the TrustMan system.

6. Conclusion

This article addresses the conceptual modeling of trust relationship between organizations as a means to contribute to the characterization of inter-organizational trust. It presents a classification of models of trust and an extensive survey of models of rational trust in organizations. The article also presents three kinds of conceptual modeling formalisms, namely: *object-based, record-based and ontology-based formalisms,* where each one is exemplified with models for trust relationships between organizations.

Object- oriented paradigm assists system developers in addressing the complexity of a problem domain by considering the problem not as a set of functions that can be performed but primarily as a set of related and interacting objects. The modeling task therefore consist of specifying for a specific context, those objects (or the class that the objects belong to), and their respective set of properties and methods, shared by all object members of the class. This modeling approach also supports the analysis of cardinalities of relationships between the objects. On the basis of these concepts, an object-based model of trust relationship between organizations is applied in our research to designing and implementing modules/functionalities of TrustMan System. Relational databases are the most commonly used type of data storage in research and practice. This is due, in large part, to the fact that the simplicity of their storage and access principles offers users greater efficiency. Also, the table-like structures map easily to most real-life data formats, such as forms and spreadsheets. Record-based models of trust relationship between organizations, developed on the bases of the concepts in relational data modeling, are presented in this article. These

proposed models are applied here in designing a relational database schema for data related to trust in an organization. The designed schema is applied in developing a database for TrustMan system.

Effectiveness of assessment of the level of trust in an organization and the acceptability of its results is greatly influenced by the common understanding of trust concepts between its involved parties. Such parties in VBEs include: trustor organizations, trustee organizations, VBE administrator organization, and other stakeholder organizations. One approach for supporting the establishment of such understanding of trust concepts is by providing these parties with an ontology describing these concepts and the terms used for various trust elements, mechanisms for assessing trust level, and applied functionality offered by the software tools used for this purpose. This article has presented an ontology-based model of trust in VBEs between the participating organizations and other actors, in order to achieve a common understanding regarding these fundamental trust concepts. Inter-organizational trust plays a key role in facilitating collaboration within the VBE. Therefore, better understanding of the concepts related to inter-organizational trust is necessary for creating successful VBEs of organizations. This article proposes models of trust relationships among organizations, constituting their related trust elements and inter-relations. As such, the article provides the stakeholders in research with a set of models to enhance the understanding and characterization of rational trust, as applied in CN.

7. References

[1] Afsarmanesh, H., Msanjila, S.S., Ermilova, E., Wiesner, S. & Woelfel, W. VBE management system. In methods and tools for collaborative networked organizations. ISBN: 978-0-387-79423-5, pg. 119-154. Springer, New York, (2008).

[2] Afsarmanesh, H. & Ermilova, E. Ontology Management for VO Breeding Environments. In the proceedings of 9th International conference on the Modern Information Technology in the Innovation Processes of the Industrial Enterprises. Pg. 124-137, Italy, (2007).

[3] Ahuja, G. Collaboration networks, structural holes, and innovation: A longitudinal study. In Administrative Science Quarterly, Vol. 45, pg. 425–55, (2000).

[4] Avila-Rosas, A. & Luck, M. A direct reputation model for VOs formation. In Multi-Agent Systems and Applications, Springer, Heidelberg, (2005).

[5] Camarinha-Matos, L. M. & Afsarmanesh, H. Collaborative Networks: Value creation in a knowledge society. In knowledge enterprise: Intelligent strategies in product design, manufacturing and management, pg. 26-40, Springer, (2006).

[6] Gambetta, D. Trust: Making and Breaking Cooperative Relations. Basil Blackwell (1988).

[7] Gloor, P.A., Paasivaara, M., Schoder, D., Willems, P. Finding collaborative innovation networks through correlating performance with social network structure. In the International Journal of Production Research, Vol 46, page: 1357-1371, Taylor & Francis, (2008).

[8] Gulati R, & Singh H. The architecture of cooperation: managing coordination costs and appropriation concerns in strategic alliances. Admin. Science Quarterly 43: 781–814 (1998).

[9] Hurmelinna-Laukkanen, P & Blomqvisit, K. Fostering R&D collaboration – The inter-play of trust, appropriability and absorptive capacity. In Establishing the foundation of collaborative networks [eds. Camarinha-Matos, L.M., Afsarmanesh, H., Novis, P. & Analide, C.] Boston, Springer, pg. 15-22, 2007

[10] Human, S.E. & Provan, K.G. An emergent theory of structure and outcomes in small-firm strategic manufacturing networks. In Academy of Management Journal, Vol. 40, No. 2, pg. 368–403, (1997).

[11] Huynh, T.D., Jennings, N.R. & Shadbolt, N.R. 'FIRE: an integrated trust and reputation model for open multi-agent systems'. In the proc. of the 16th European Conference on Artificial Intelligence (ECAI), Kluwer Academic Publishers, Valencia, pp.18–22. (2004).

[12] Keen, P. G. W. Competing in the chapter 2 of the internet business: Navigating in a new world. (www.peterkeen.com/delft2.htm), 1999.

[13] Kini, A. & Choobineh, J. Trust in electronic commerce: definition and theoretical considerations. In the proceedings of the 31st Annual Hawaii International Conference on System Sciences, Kohala Coast, Hawaii, pp.51–61. (1998).

[14] Korba, L. & Song, R. A Reputation Evaluation System for Mobile Agents. In the in Proceedings of the 5th International Workshop on Mobile Agents for Telecommunications Applications. Marrakech, Morocco. October 8-10, 2003.

[15] Lucas, L.M. The impact of trust and reputation on the transfer of best practices. In the Journal of Knowledge Management, Vol. 9, Issue 4, pg. 87-101, Emerald Group Publishing Limited, 2005

[16] Maciaszek, L.A. Requirements analysis and system design. ISBN: 978-0-321-44036-5. Third edition. Pearson Education Limited (2007).

[17] Msanjila, S.S. On inter-organizational trust engineering in networked collaboration – modeling and management of rational trust. ISBN: 13:9789057761966, IPSkamp drukkers, Amsterdam, The Netherlands, 2009.

[18] Msanjila, S.S., Afsarmanesh, H. FETR: A Framework to Establish Trust Relationships Among Organizations in VBEs. In the International Journal of Intelligent Manufacturing; Special issue: Trust, Value Systems and Governance in Collaborative Networks. ISSN 0956-5515, Springer, (2008a).

[19] Msanjila, S. S. & Afsarmanesh, H. Trust Analysis and Assessment in Virtual Organizations Breeding Environments. In the International Journal of Production Research, ISSN (print) 0020-7543, pg. 1253-1295, Taylor & Francis. (2007a).

[20] Msanjila, S.S. & Afsarmanesh, H. Modeling trust relationships in Collaborative Networked Organizations. In international Journal of Technology Transfer and Commercialization, ISSN (print): 1470-6075, Vol. 6, No. 1, pg. 40-55, Inderscience, (2007b).

[21] Msanjila, S. S. & Afsarmanesh, H. HICI: An approach for identifying trust elements – The case of technological perspective in VBEs. In proceeding of International conference on availability, reliability and security (ARES-2007), pg. 757-764, Vienna, (2007c).

[22] Lee, M.K.O. & Turban, E. A trust model for consumer Internet shopping. In the Journal of E-Commerce, Vol. 6, No. 1, pg. 75-91, (2001).

[23] Pinyol, I., Sabater-Mir, J. & Cuni, G. How to talk about reputation using a common ontology: from definition to implementation. In the proceedings of 6th International joint conference on Autonomous Agents and Multi-agent Systems – W20: Trust in Agent Societies, pg 90-101. Hawaii, (2007).

[24] Resnick, P. & Zeckhauser, R "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputatoin System." In proc. of NBER Workshop on Empirical Studies of E-Commerce. (2000).

[25] Sharratt, M. & Usoro, A. Understanding Knowledge-Sharing in Online Communities of Practice. In the electronic journal of management, vol.8, no 2. pg. 187-196, (2003).

[26] Szulanski, G. Unpacking stickiness: An empirical investigation of the barriers to transfer best practice inside the firm. In Academy of Management Best Papers Proceedings, pg. 437–41, (1995).

Biography:

Dr. ir. Simon Samwel Msanjila graduated BSc. Computer Science in 2001 from the University of Dar es Salaam, Tanzania; MSc. in Systems Engineering in 2004 from the Delft University of Technology, The Netherlands; and PhD in Computer Science in 2009 from the University of Amsterdam, The Netherlands. Currently, he is employed as a Senior Lecturer at the Mzumbe University in Morogoro, Tanzania. He is also the head of information and communication technology department. In addition to teaching a number of courses in Computer Science disciplines, he conducts research focusing on the establishment and management of collaborative networks of organizations. In the area of collaborative networks, Dr. Msanjila focuses on the management of information to support business operations conducted within these networks. One fundamental aspect of interest to him is the management of information to support the analysis and measurement of rational trust in organizations that are participating in business collaborative networks. Dr. Msanjila is also involved in research focusing on designing of infrastructures and systems to support enhancing professional active life of senior professionals (retired and retiring professionals). Currently he is performing research on development of a collaborative ICT infrastructure supporting the provision of online - live and offline - HIV/AIDS advisory services to students and younger generation in Tanzania. Dr. Msanjila has authored one book titled "On inter-organizational trust engineering in networked collaboration". He has also published a more than 40 papers in journals, as book chapters, and in peer reviewed–book format international conference proceedings.