International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:10, 2015

A Tool for Rational Assessment of Dynamic Trust in Networked Organizations

Simon Samwel Msanjila

Abstract**—**Networked environments which provide platforms for business organizations are configured in different forms depending on many factors including life time, member characteristics, communication structure, and business objectives, among others. With continuing advances in digital technologies the distance has become a less barrier for business minded collaboration among organizations. With the need and ease to make business collaborate nowadays organizations are sometimes forced to co-work with others that are either unknown or less known to them in terms of history and performance. A promising approach for sustaining established collaboration has been establishment of trust relationship among organizations based on assessed trustworthiness for each participating organization. It has been stated in research that trust in organization is dynamic and thus assessment of trust level must address such dynamic nature. This paper assesses relevant aspects of trust and applies the assessed concepts to propose a semi-automated system for the management of Sustainability and Evolution of trust in organizations participating in specific objective in a networked organizations environment.

Keywords**—**Trust evolution, trust sustainability, networked organizations, dynamic trust.

I. Introduction

NETWORKED organizations refers to an alliance of legal firms that has come together virtually for the purpose of joining their efforts and sharing competences and resources for the purpose of jointly executing an opportunity that have characteristics for which none of the involved organizations could respond alone. The emergence of networked organizations as new form of virtual firms comes as benefits of the increasing innovation and advances of digital technologies and communication technologies for which information can be exchanged irrespective of location and time. A number of different forms and types of such networked organizations are mentioned in literature, a few to mention are collaborative networks, virtual organizations, virtual organizations breeding environments, virtual enterprises, among others [1].

It has been observed that organizations nowadays need to collaborate with others for the purpose of addressing complex and bigger opportunities which also have proven to be so volatile with time. The volatility comes in sense that customer requirements for the needed products and services in today's businesses are changing very frequently. As such business organizations now see the approach to push others outside the market in competition manner as no longer an option rather pulling others closer for the purpose of enhancing the chance to collaborate in future as the optimal option. However, it has proven to be a challenging factor for organizations to configure the needed collaboration particularly when such a network needs to be established in a short time to meet the emerged opportunity. Further, even after configuring the network the sustainability of the operations in such collaboration need to be assured which remains to be a challenge.

It has been observed from literature that smooth configuration and operation of the networked organizations needs to be supported with properly established trust relationships among partners as a bonding factor for enhancing co-working. It has been further observed that there are a number of forms of trust that can be established such as bilateral trust, subjective trust, objective trust, reputation based trust, and rational trust among others. Of these types of trust the rational trust among organizations which is established on the basis of factual performance data of each involved organizations has been mentioned to be the sustainable bonding factor for business collaboration [4]. Established rational trust among organizations using mechanisms that are formulated based on measurable factor can enhance partner's confidence on a specific partner of the networked organizations environment to execute its assigned roles appropriately and thus contribute in achieving the common network goal(s).

It is acknowledged that variation of perceptions on trust to different actors exists. Consequently, different definitions of trust are developed for varying use purposes in distinguished environments. *As far as networked organizations environment is concerned in this paper we adopt the definition of rational trust in an organization as an objective-specific confidence of a trustor in a trustee, based on the results of rational (fact-based) assessment of trust level of the trustee* [3]. Considering our developed mathematical based mechanisms [2], the main input into trust analysis is measurable organization's performance data. The factual performance data obtained from the analysis of objective trust plays a significant management role towards various reasons driving the collaboration.

As stated earlier, networked organizations are configured in different format. Considering short time as a feature and objective specific collaboration as another feature we can define, as so popular in literature, the so called Virtual Organization (VO). A VO is defined as an organization involving legally detached and disseminated entities mostly firms and requiring digital and information technology to support their co-work and information exchange or simply

S. S. Msanjila is with the College of Business Education holding the post of a Deputy Rector for Academic, Research and Consultancy, P.O.Box 1968, Dar es Salaam, Tanzania (e-mail: s.msanjila@cbe.ac.tz).

communication. As such VO does not represent a firm's attribute but can be considered as a different organizational form.

In some literature, it has been observed that partners of virtual organizations must be selected from a well-established long term strategic alliance of organizations. A Virtual organizations Breeding Environment (VBE) is mentioned for this purpose. AVBE has been defined *as association of organizations and their related supporting institutions, adhering to a base long term cooperation agreement, and adoption of common operating principles and infrastructures, with the main goal of increasing their preparedness towards rapid configuration of temporary alliances for collaboration in potential VOs*. Thus the term VO is used to describe a network of independent firms that join together, often temporarily, to produce a service or product for a specified customer. VOs are often associated with such terms as virtual office, virtual teams, and virtual leadership. The ultimate goal of the VO is to provide innovative, high-quality products or services instantaneously in response to customer demands.

Organizations collaborate and cooperate for a number of reasons including enhancing preparedness, saving time and decreasing development process, sharing costs and risks with partners, improving resource utilization, and gain access to new markets through partnership [5]. For these advantages of collaboration to be gained it has been stated in research and observed in practice that participating organizations must rationally trust each other throughout the collaboration period. However, although can be established at the VO creation, trust of the VO partner does not remain static, but evolve depending on many influencing factors including actual partner's performance in the VO. The dynamic trust can result in either rise or fall of the trust level of a specific partner with respect to time. It is, therefore, important to note that trust of an organization is dynamic and evolves over time. The dynamicity nature of trust needs comprehensive analysis and measurement approaches, particularly for the collaboration which is already in progress. The dynamic nature of trust cannot be assessed conventionally, especially for short-term collaborations, because conventional approach to build trust among business partners has proven to be inefficient [6]. Such convectional approach in building trust, is what we refer to as *subjective trust*. Therefore, when subjective trust is inefficient, then object trust suits better and particularly where there is objective collaboration and collaborating partners have little knowledge about each other.

II. Organizational Trust and Trust Assessment

A. Subjective and Objective Trust

A prerequisite to configure a consortium in form of a networked organization such as a virtual organization (VO) has been observed to be creating trust among its involved organizations. Nevertheless, creating trust among organizations in a large-size network such as the one involving a number of tens of organizations, whose members do not know each other well is challenging [7]. Traditionally, trust among organizations was only established "bi-laterally" and subjectively in most cases applying reputation and recommendation data from others. Networked organization environments however, applying traditional approaches for creating bilateral trust among organizations has proven to be challenging mostly due to the following observations: on one hand it is hardly feasible for a trustor organization to collect reputation data or peer opinions about the trustworthiness of a trustee organization, with whom it had never interacted before, and on the other hand it is hardly feasible to rationally reason on the trustworthiness of organizations based on subjective data [7]-[10].

In order to support the creation of trust among organizations in networked organizations environments, an objective trust based on rational (fact-based) approach is suggested [9]. This approach applies formal mechanisms to assess trust of organizations. These mechanisms are derived applying measurable trust criteria such as the past performance, the achieved results, etc. With this approach an organization can rationally trust others based on facts about their trust level. Thus, trust level of organizations can be properly assessed through their trust criteria which can be supported by some rational reasoning based on the mathematical equations.

Subjective trust is the most popular form of trust that has been adopted and practiced for smoothing interactions among individuals. However, today's collaboration among organizations has become a fundamental approach for co-working in business, such as joining initiatives and efforts for the purpose of enhancing competitive power in the market. Thus applying subjective trust concept in formal collaborations is difficult to assure success as it lacks the reasoning approach and mechanism on the results of the assessment of trust level of organizations and thus rational trust analysis is now becoming popular [1]. Subjective trust is created based on qualitative data and is an opinion-based. Some fundamental sources of information for creating subjective trust among parties include: experience and knowledge of the trustor on the trustee, recommendations of third parties on the trustee, previous interactions, reputation of the trustee, etc. [9].

Rational trust is created based on quantitative data and is a fact-based. The main source of trust related data is the organizational performance which is accumulated in the past from different activities participated, both in collaboration with other partners, and also, as an individual organization. Since rational approaches for assessing trust level of organizations apply formal mechanisms, such as mathematical equations, they provide some formal reasoning means on the resulted trust level [8]. In addition to the difference in approaches for assessing trust level and their sources of data as shown in Table I, subjective and rational trust also differ in relation to the "boundaries" to which they apply. The challenging aspect is related to where do trust boundaries start and end for daily interactions among actors for both rational and subjective trust.

TABLE I
DIFFERENCE BETWEEN SUBJECTIVE TRUST AND RATIONAL TRUST

Subjective trust	Rational Trust
The creation of trust is traditional and proven.	The creation of trust is emerging and unproven.
Mechanisms for assessing the level of trust are known and informal.	There is lack of mechanisms for assessing the level of trust and formal ones are needed.
The assessment applies opinions of others.	The assessment is based on rational data.
The trust related data and their sources are known and are proven.	The trust related data and their sources are difficult to define and need verification.
Does not necessarily need tools for supporting related processes.	Needs tools due to the urgency for processing a large amount of data.
Trust criteria are mostly known and static.	Trust criteria are not known and are dynamic.
Less interferences in establishing trust relationship.	Other stakeholders must be involved while establishing trust relationships.

B. Trust Boundaries

1. Boundaries for Subjective Trust

Boundaries for subjective trust can be addressed in relation to the transitivity and propagation nature of trust among the involved actors. Subjectively, trust transitivity means, for example, that if "Alice" trusts "Bob" and "Bob" trusts "Eric" then "Alice" trusts "Eric". This assumes that Bob actually tells Alice that he trusts Eric, which is called a recommendation. In social and individual interactions, in which subjective trust is mostly practiced, trust can be assumed as transitive. This is because trust among individuals participating in these interactions is mostly created based on opinions from others. The opinions from others who trust the specific individual are used to create trust to a new trustor. Thus subjective trust is transitive.

It is common to collect advices from several sources in order to be better informed when making decisions. In other words, it is also common to collect several recommendations in order to convince the trustor, such as for job application, on the trustworthiness of the trustee. When the trustor has different sources of recommendations from which he/she can create trust to the specific trustee a specific characteristic of trust transitivity namely parallelism emerges. Since subjective trust is transitive the complex issue is at which point does the propagation ends? The point at which trust propagation ends defines the trust boundary and it is not clear which factors can indicate such a boundary. As such even the trust boundary itself is subjective from one trustor to another.

To represent the boundary for transitivity of subjective trust, assume E is an entity representing an actor such that E_1 trusts E_2; E_2 trusts E_3;. .. E_j trusts E_{j+1}. Assume also TR refers to trust relationship and TL refers to trust level of trustee. Trust boundary TB for E_1 can be represented in mathematical logics as shown in (1):

$$\forall(E_1, E_j, E_{j+1}) \in E, \exists TR(E_1, E_{j+1}) \Leftrightarrow \{\exists TR(E_1E_2) \wedge \exists TR(E_2E_3) \wedge .... \wedge \exists TR(E_j, E_{j+1})\} \wedge \{TL_{E_2} \leq TL_{E_3} ... \leq TL_{E_{j+1}}\} \quad (1)$$

2. Boundaries for Rational Trust

It can be shown that trust is not transitive for objective specific collaborations and transactions for which rational trust is mostly practiced. For example, the fact that Alice trusts Bob to look after her child, and Bob trusts Eric to fix his car, does not imply that Alice trusts Eric for looking her child, or for fixing her electric lamp. This is because the trust objectives in the two cases differ. Rational trust is created based on facts and applying formal mechanisms in which different cases will have different preferences. As such the value of trust level in this case is not absolute and cannot be transferred to different cases. This is the reason why rational trust fits better than subjective trust for smoothing organizations' objective specific collaborations. Thus rational trust is not transitive.

Rationally, trust boundary does not exist since trust is created based on the preferred perspective. Different trustor can prefer different perspectives to trust the same trustee. When the same set of trust criteria is preferred for all trustors then at the end the same trust level shall be achieved independent of the trustor. Therefore, rational trust does not propagate among involved actors and thus all trustors shall trust their respective trustee based on their own preferred perspective.

C. Trust Relationships

One important strategy that is necessary for long-term strategic alliances of organizations is to focus on organizational preparedness to enhance their chances of participating in organizational short-term networks such as VOs. Organizational strategies must therefore properly address the notion of collaboration with other business partners. In addition to acquiring resources, knowledge and competencies, a crucial aspect of the preparation process involves establishing trust relationships with potential business partners in order to smoothen possible collaboration. There are two kinds of trust relationships between organizations that can be established in networked organizations environments, namely:

- ***Short-term trust relationships***: established to facilitate co-working between organizations that will exist for a relatively short period of time, e.g. collaborations in VOs.
- ***Long-term trust relationships***: established to facilitate co-working between organizations that will exist for a relatively long period of time, e.g. cooperation in Long – term networked organizations environments.

Consideration of a large number of specific fundamental aspects is necessary when addressing trust between organizations in networked organizations environments. As demonstrated in our previous work, inter-organizational trust is characterized as a multi-objective, multi-perspective, and multi-criteria subject [2]. It is a challenging task to comprehensively cover all these specific fundamental aspects of inter-organizational trust and thus use them to facilitate the establishment of trust relationships between organizations. A single specialized approach, such as based on reputation of organizations, security of systems, etc., cannot adequately cover all fundamental aspects of trust that need to be considered while establishing trust relationships between organizations in networks of organizations. Accordingly, a

generic but comprehensive and structured approach must be designed that will support the realization of inter-organizational trust relationships in these environment. A multi-perspective and multi-criteria approach is proposed in [2]-[8] which consider a large set of criteria for organizations to assess the needed trust.

A number of specific steps must be taken into account in order to characterize the planned relationships and prepare the involved organizations on a number of essential aspects in establishing their goal-oriented trust relationships. In order to effectively establish trust relationships between organizations applicable to different domains a number of steps to follow are proposed in previous work [11]. These steps for establishing trust relationships are the following as further presented in [11]:

- Assessment of level of trust in organizations,
- Validation of trust level results based on the analysis of evidence of validity of the trust related data,
- Presentation of levels of trust in organizations and related trust concepts as easy and understandable as possible to involved organizations,
- Creation of trust between organizations to support the launching of the intended trust relationships by providing sufficient information based on a number of trust aspects.

A trust relationship in our work is therefore defined as a state of connectedness between organizations, or a state involving mutual dealing between organizations both based on factual based assessed trustworthiness of each involved partners. Thus trust relationship refers to the state of connectedness between a trustor and a trustee whose intensity is characterized and based on rational trust level.

D. Static, Dynamic, Base and Specific Trust

Various forms of trust can be characterized that are being practiced by organizations in facilitating collaboration and co-working. In our research we have characterized them into static trust, dynamic trust, base trust and specific trust whose definitions are provided here.

- Static trust is a form of trust which is assumed to remain constant, uniform or unchanged with time. With this form of trust it is assumed that the assessed trust level of involved organizations shall not change as they keep collaborating in future.
- Dynamic trust is a form of trust which is assumed to change with time during the collaboration. It is assumed that trust level shall change due to achievements and failures in on going activities within the collaboration and thus there is a need for assessing trust level from time to time.
- Base trust is defined to be the minimum level of trust that an organization must achieve to be invited and accepted in the collaboration.
- Specific trust is a form of trust which is assessed and established to meet a very specific objective and only during the life time of the objective.

III. Trust Analysis and Management Systems

A. Trust Assessment Mechanisms

Perceptions of trust correspond with both the nature of the purpose of its application, as well as the actors involved. Thus, the purposes for establishing trust differ among different practices. For each specific practice in which a particular group of actors is involved, trust is interpreted and perceived differently. In our previous research we have classified into five perspectives: Technological perspective (Tech), Social perspective (Soc), Structural perspective (Str), Managerial perspective (Man), and Economical perspective (Eco). Furthermore, in order to address the differences in trust perceptions, a rational trust level assessment approach is required to both assist the measurement of trust level of organizations and reasoning of the results.

In order to "rationally" assess the level of trust in organizations, a series of fact-based trust criteria are applied. Using an empirical study of running networked organizations, as well as a survey of past research, our research has identified a substantial number of measurable criteria (trust criteria) that act as indicators of trust assessment [14]. It has also been revealed that the influence of a trust criterion on the level of trust can be either positive or negative, depending on its behavior in the environment. Furthermore, the behavior of each trust criterion changes over time and causally influences other criteria. Causal influences can be studied by applying concepts from system dynamics [12], and the results of a causal analysis can be visually represented in a so-called "*causal diagram*". Such results can also be translated into mathematical equations that reflect the inter-relations among trust criteria [8]. The formulated equations comprise the base for the mechanisms that have been designed in the TrustMan system, as presented in Section IIIB, for assessment of the level of trust in organizations [8]. As implemented in the TrustMan system, basically, mechanisms to calculate the final comparative trust score for an organization is formulated as the computation of an average of weighted scores of all trust perspectives (2) where the weight is between 0 and 1, and the total weights applied for all parameters is 1. The following abbreviations are used in all subsequent equations: **TL** (trust level), **S** (score), **per** (trust perspective), **IF** (intermediate factor), **W** (weight), and **Avg** (average).

$$TL = Avg[(W_{Tech} * S_{Tech}),(W_{Soc} * S_{Soc}),(W_{Str} * S_{Str}),(W_{Man} * S_{Man}),(W_{Eco} * S_{Eco})] \quad (2)$$

The weights of parameters used in the equations are dynamically specified by the trustor organization depending on its trust objective during the assessment of trust level. If these weights are not specified by the trustor then the TrustMan system assumes uniform weights for all parameters in each equation. The score for each trust perspective is calculated as a weighted average of the score for all intermediate factors as shown in (3).

$$S_{per} = \frac{1}{n} \sum_{i}^{n} W_{IF_i} * S_{IF_i} \quad (3)$$

where "n" refers to the number of defined intermediate factors for the trust perspective. The score for the intermediate factors is calculated as a function of trust criteria and known factors as shown in (4). These equations are formulated from the results of causal analysis.

$$S_{IF} = f[trust\_criteria, known\_factors] \quad (4)$$

B. Static Trust Management System

Objective trust for organizations presented in Section IIB, requires a proper conceptualization and modeling in order to address its measurement factually. The varying perception of trust accounts for a complex modeling of trust measurement. When the objective trust is a concern, then formal approaches are important so that trust can be processed and executed by computer systems. The rational results from such kind of measurement can be used to objectively configure a new consortium, by selecting members from long-term strategic alliance of organizations. In a study conducted by [14], a HICI (Hierarchical, Impact and Causal Influence) approach was used to model trust measurement. The assessment of trust employed data from organization's performance for every organization in a networked environment. The automation of assessment mechanisms were presented through Trust Management (TrustMan) system. The TrustMan system is prototypical software that was used to configure the new short-term organizational consortiums such as VOs, for a new business opportunity realized [13]. Such consortiums are formed based on specific objectives, by selecting partners from existing members of the networked environment, whose trustworthiness are objectively assessed to be satisfactory.

C. Dynamic Trust Management System

The evolution of trustworthiness can hardly be assessed and analyzed precisely without a semi-automated system. This is due to the fact that the analysis is complex requiring analysis of large set of trust criteria and computing large volume of data. The functionalities of such a system for the purpose of supporting the assessment and management of dynamic trust in networked organization environments are presented in this section. The system is referred to as Trust Sustainability and Evolution System (TrustSEv System).

IV. The TrustSEv System

The TrustSEv system provides a number of functionalities while interoperating with the TrustMan system to support organizations to assess and analyze the evolution and sustainability of trust as part of management of dynamics of trust level of organizations. Table II summarizes the services provided by the TrustSEv system.

V. Architectures of the TrustSEv System

The TrustSEv system provides services specified in Table II, through implementation of two architectural styles, namely: (1) the Interoperability Architecture, and (2) the Four-layer Componential Architecture. In order to provide the promised services systematically, accurately and comprehensively, the TrustSEv system interacts with TrustMan system as illustrated in Interoperability Architecture (Fig. 1).

Such interactions are mainly for two purposes, namely; (1) acquiring trust values and data on trust level from TrustMan system and (2) supporting human user access to deliver the requested services. The further purpose behind this TrustSEv interoperability architecture is to guide developers during the implementation of modules supporting the required external interactions. External interactions into TrustSEv system are supported by internal components classified into three groups, namely: (1) access verification, (2) service structure, and (3) service delivery. The components for access verification provide administrative functionalities to both human and system users interacting with TrustSEv system. They also classify the services that can be requested based on privileges for each specific user in the system. The components for service structure provide the internal mechanisms, namely the choreography related to business logic functionalities based on service request. The components for service delivery provide requested response to users, or when failure a feedback and cause of failure.

TABLE II
Services Provided by the TrustSEv System

Service Name	Service Description
For input of basic information related to VO	This service supports coordinator to enter basic information related to partners of the said collaboration. The coordinator is appointed among partners who can solely be a prime partner.
For input trust values and trust level	This service supports requesting trust values and related data from *TrustMan* system after activation by the participant observer into *TrustSEv* system. A participant observer is a human user (say, coordinator). This is an administrative service and it is accessed by the coordinator.
For forecasting target goals for the next period of assessment	This service provides target agreements customizable to every participating partner. Since trust is dynamic, the target is a range defined by lower limit and upper limit trust values, in which a healthier partner's trust level is optimally allowed to oscillate.
For assessment of sustainable trust value and trust level	This service provides a mechanism for assessing trust level of partners. This is a limited administrative service and is thus accessed by the coordinator and the partner.
Defining, authorizing and assigning rights to other users	The service supports defining user access levels for partners and guests with different privileges. It is a highly administrative service and thus only coordinator can access it.

The Four-layer Componential Architecture of TrustSEv system (Fig. 2) comprises of four layers, namely: (1) the presentation layer, (2) the process layer, (3) the description layer and (4) the message layer. Presentation layer links process layer and human user. It is a platform where data/information from human user/TrustSEv system is exchanged in human readable form. Consequently, it deals with transformation of data from process layer into human readable text. Further, in order to protect sensitive information from exposure to the third party, the web services are designed to support user access rights in three levels, namely, public, restricted and protected interfaces.

Process layer is the core heart of the business logic processing in which various modules and components are executed, for services provision. The process layer is

constituted of process scheduling referred to as orchestration and choreography. The description layer provides grammatical and dictionary-like specifications of services in order to create supportive invocation by external and remote components, and employs Web Services Description Language (WSDL). The message layer is responsible for specifying communication protocols among both, the internal and external components. The layer controls invocation protocols internally, and communicates externally by using Simple Oriented Access Protocol (SOAP) standard protocol for web services.

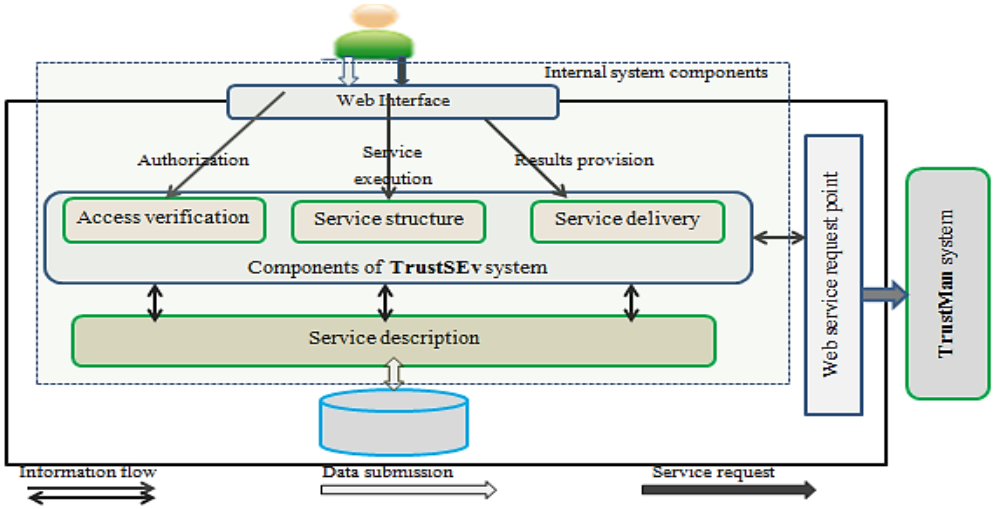

Fig. 1 Interoperability Architecture of TrustSEv System

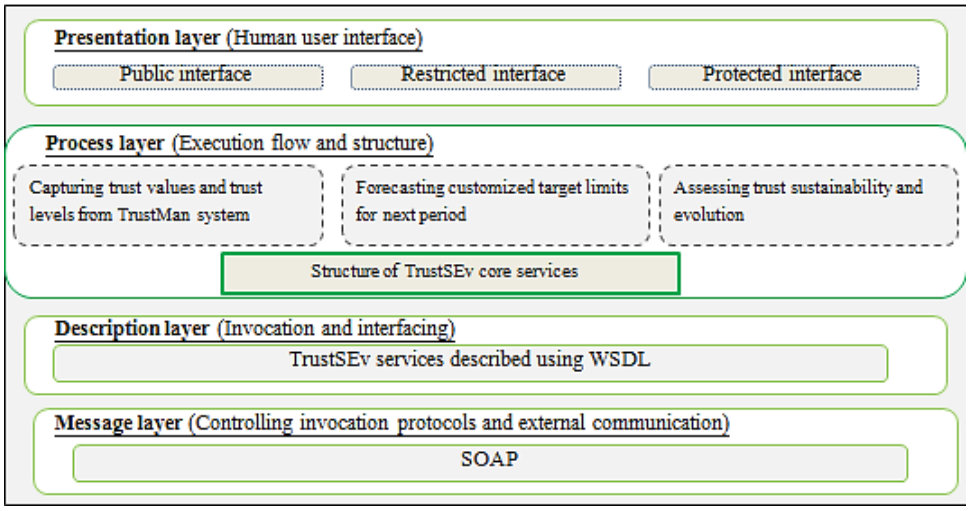

Fig. 2 Four-layer Componential Architecture of the TrustSEv system

VI. Example Service: Forecasting Trust Target Goals

This service supports the collaborating partners to set target goal on trust values that each partner must sustain in order to remain trustworthy in collaboration. For example, in Fig. 3 the coordinator was forecasting target goals for year 2013 using organization's performance data of the year 2012.

For instance, the organization with Identity (ID 51) had its target goal in terms of trust value set to lie between 2.063 and 2.641 inclusive for the year 2013. Then after a lapse of a two-six month period, organization's performance data for each partner is submitted to the coordinator. Then the values are fed into TrustSEv system for assessment, by diagnosing to whether the current trust value lies within preset custom target goals. After assessment, the partner with ID number 51 had its performance score in 2013 found to be 2.271, which implies that such partner maintained its trust level within the acceptable limits. Contrary, a partner with ID number 54 had its target goal preset to lie between 1.896 and 2.474 inclusive, but managed only to score a trust value of 1.854. The partner had failed to maintain its trust level. Such failure implies partner's low ability to collaborate, because it cannot be trusted in executing the required duties. Since the partner has starved, then it is recommended for replacement. Such replacement of the failed partner accounts for overall change in trust level set by the network of partners since the assessed

trust level is comparative value. The change brings new reconfiguration in trust value, termed as trust evolution.

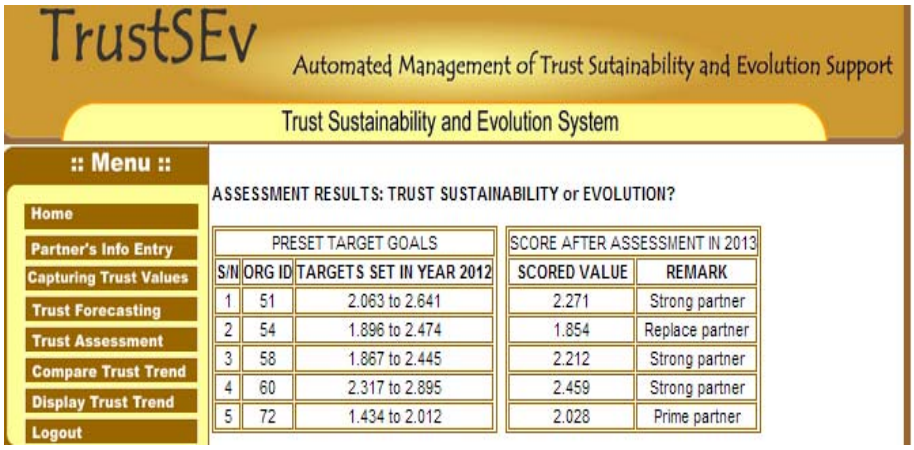

Fig. 3 Assessment on trust evolution in TrustSEv system

VII. Conclusion

This paper has presented the assessment and analysis of evolution and sustainability of dynamic trust in networked organizations environment. The paper has also presented various aspects of subjective trust which are compared to aspects of objective trust. The paper proposes the adoption of rational trust and related assessment approaches for assessing and managing trust in networked environments to ensure smooth evolution and enhance sustainability during the time of collaboration.

References

[1] Camarinha-Matos, L. M. & Afsarmanesh, H. Collaborative networks: a new scientific discipline. *International Journal Intelligent Manufacturing*, 16, 2005, pp. 439–452.

[2] Daudi, M., Msanjila, S. S. Modeling of Evolution and Sustainability of Rational Trust in Dynamic VOs. In Camarinha-Matos, L. M., Scherer,R. J. (Ed) *PRO-VE 2013, IFIP AICT,* 408, 2013, pp. 548-555, Springer, Heidelberg.

[3] Msanjila, S. S. & Afsarmanesh, H. On development of TrustMan system assisting configuration of temporary consortiums. *International Journal of Production Research*. 47(17), 2009, pp. 4757 -4790.

[4] Msanjila, S. S. Engineering the Evolution of Organizational Trust in Operating Virtual Organization. *International Journal of the Academy of Organizational Behavior Management (IJAOBM),* 1, ISSN: 1927-565X, 2012, pp. 120-138.

[5] Nami, M. R. & Malekpour, A. Toward Autonomous Virtual Organizations". *International Journal of Hybrid Information Technology*. 2(1), 2009, pp. 57-64.

[6] Wehmeyer, K. & Riemer, K. Trust-building potential of coordination Roles in virtual organizations. *In The Electronic Journal for Virtual Organizations and Networks*, vol. 8, 2007.

[7] Afsarmanesh, H., Camarinha-Matos, L. & Msanjila, S.S. Virtual organizations breeding environments: key results from ECOLEAD. *In the proceedings of International conference on Cost Effective Automation in Networked Product Development and Manufacturing* – IFAC-CEA'2007. Monterey, Mexico, 2007.

[8] Msanjila, S. S. & Afsarmanesh, H. Trust Analysis and Assessment in Virtual Organizations Breeding Environments. *International Journal of Production Research*, ISSN (print) 0020-7543, 2007, pp. 1253-1295.

[9] S. S. Msanjila. On inter-organizational trust engineering in networked collaboration: modeling and management of rational trust. IPS drunkkers publishers, ISBN 9789057761966, Amsterdam, 2009.

[10] Castelfranchi, C. & Falcone, R. Trust Is Much More than Subjective Probability: Mental Components and Sources of Trust. *In proceedings of the 33rd Hawaii International Conference on System Sciences*. Hawaii, 2000.

[11] 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, 2008.

[12] Kirkwood, C. W. System Dynamics Method. Ventana System Inc. 1998.

[13] Msanjila, S.S. & Afsarmanesh, H. Specification of the TrustMan system for assisting management of VBEs. *Lecture notes of computer science series*, LNCS 4657, Springer, 2007b pp. 34-43.

[14] 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*., 2007a, pp. 757-764, Vienna.