International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:2, No:5, 2008

Trustworthy in Virtual Organization

Abdolhamid Fetanat, and Mehdi Naghian Feshaareki

***Abstract*—**In open settings, the participants in virtual organization are autonomous and there is no central authority to ensure the felicity of their interactions. When agents interact in such settings, each relies upon being able to model the trustworthiness of the agents with whom it interacts. Fundamentally, such models must consider the past behavior of the other parties in order to predict their future behavior. Further, it is sensible for the agents to share information via referrals to trustworthy agents. In this article, trust is a bet on the future contingent actions of others" and enumerates six major factors supporting it: (1) reputation, (2) performance, (3) appearance, (4) accountability, (5) precommitment, and (6) contextual facilitation.

***Keywords*—**Trustworthy, trust, virtual organization.

I. Introduction

THE concept of trust in decentralized and distributed organizations has been an important area of recent research in sociology, cognitive science and artificial intelligence. Trust is positive expectations of positive actions by others, and is important to well-functioning organizations of all sorts. Trust facilitates the effectiveness of organizations. A focus on trust leads to a more humanistic view of individuals within organizations than that of the traditional managerial psychology of humans solely as input-output devices whose performance must be monitored and measured. In virtual organizations, due to the high uncertainty about quality and reliability of the products and services offered by others, it is crucial for agents to compute the trustworthiness of the other agents before initiating any service request. Similar considerations apply in Web-based information systems, in general: agents must be able to compute how much trust to place in others with whom they might have had no prior experience.

The trust as a cognitive concept in dynamic, decentralized and distributed systems will be effective and critical role. If the organization will be considered as a sociality network then the trust is main glue for avoid of chaos. An agent-based referral social network as a virtual organization is a multiagent system whose member agents give referrals to one another (and are able to follow referrals received from other agents). To do so effectively presupposes certain representation and reasoning capabilities on the part of each agent. Each agent has a set of acquaintances, a subset of which is identified as its neighbors. The neighbors are the agents that the given agent would contact and the agents that it would point (refer) others to. An agent maintains a model of each act in a trustworthy manner and to refer to other trustworthy agents, respectively.

New technology changes the form of virtual organizations operations. So it is natural to ask how trust is affected by the advent of the technologies and practices of virtual organizations, as it is affected by online security practices [6]. On the one hand, virtual organizations should be more efficient organization, and people trust more in well-run, efficient processes. The virtual organizations could enable organizations to evade responsibility for their actions by imposing new barriers to agents, restricting access to information more, falsifying information more easily, and providing a new set of excuses for inefficiency. Some extremists [10] claim that most technology cannot be trusted, but few agent agree. So the issue needs to be examined at length.

There is not consensus in the literature on what trust is; it is recognised as an important and complex subject relating honesty, truthfulness, competence, reliability, etc. of the trusted person or service. One of the influential works towards a practical definition of trust is given by Gambetta [8]: "When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly, when we say that someone is untrustworthy, we imply that that probability is low enough for us to refrain doing so." Gambetta's definition stresses that trust is fundamentally a belief or estimation, which has inspired the use of subjective logic as a way of measuring trust [11].

In this paper, we focus that Trust should be defined as "a bet on the future contingent actions of others" and enumerates six major factors supporting it: (1) reputation, (2) performance, (3) appearance, (4) accountability, (5) precommitment, and (6) contextual facilitation[17]. We show that these factors will be growing in referral virtual organization' the reputation factor is not much influenced by whether organizations is digital or not, but reputation system provide the mechanisms that support finding trust estimations based of evidence theory and is a main component in referral distributed organization. Performance and accountability are supported by virtually any organizations: Past performance of organizations (demonstrating that procedures are being followed) and lines of accountability (indicating that recourse is available for fixing problems) are almost always present. But virtual organization can improve performance and accountability by exploiting its ability to store extensive documentation. For instance, virtual organizations can keep records (while removing identifying information to maintain

privacy) to demonstrate that agents are being treated fairly and equally. They can also track agent interactions and requests to show that procedures are functioning properly.

Appearance is related to the user-friendliness of virtual organizations, and this can be ensured by good human-interface design for the software, with phone numbers and email addresses of human contacts provided in case of problems. Precommitment (fulfilling initial steps to build trust in completing a full promise) can be accomplished in virtual organizations by offering receipts, certificates, and other documentation at milestones while providing a service. Finally, contextual facilitation is the "culture of trust" cultivated by a organizations by treatment of its agents, and is only indirectly related to virtual organizations through its performance.

We also distinguishes between instrumental trust (related to specific goals), axiological (based on moral expectations), and fiduciary (based on legal or quasi-legal obligations). But we mention that the referral social network is generally evolving to every type of trust. In this context, instrumental trust for access to the shared situation awareness and deep understanding of customer intention makes moral claims and fulfill legal obligations for referral query are need.

II. Virtual Organization and Edge Organization

Virtual organizations are dynamic collaborative collections of individuals, enterprises, and information resources [5]. Traditionally such collaborative activities are focused on data sharing and computation. Virtual organizations, whether business or scientific, have key properties that distinguish them from traditional IT architectures: 1) Autonomy**.** The members of a Virtual organization behave independently, constrained only by their contracts.2) Heterogeneity**.** The members of a Virtual organization independently designed and constructed, constrained only by the applicable interface descriptions. 3) Dynamism. The configuration of a Virtual organization changes at runtime as members join and leave. 4) Structure. Virtual organizations have complex internal structures, reflected in the relationships among their members. We propose that the edge structure for every virtual organization and referral network will be provide the communication agent backbone such that the trust and trustworthy will be reinforced.

Now let us consider some specifics of trust in virtual organization. Virtual organization usually strives to increase accessibility of the organization to the agents, and this will increase trust in the organization by Sztompka's factors of appearance and performance. The performance factor arises in Virtual organization as a referral network. In fact, the Virtual organization has the edge structure that represents a fresh approach to organizational design. The edge organization reaches of Computational Organization Theory (COT) and Computational Social Science (CSS). The edge approach opposite to the hierarchical structure in which the knowledge and every competency will be moved and diffused, simplicity. Computational Organization Theory (COT) and Computational Social Science (CSS) are emerging, multidisciplinary fields that integrate aspects of artificial intelligence, organization studies and system dynamics/simulation [32]. The edge implies adoption of an edge organization, with greatly enhanced peer-to-peer interactions. Edge organizations also move senior personnel into roles that place them at the edge. They often reduce the need for middle managers whose role is to manage constraints and control measures. Power and knowledge to the edge, when fully achieved in each of the domains of Virtual organization as decentralized and distributed organizations, provides the conditions that allow to reach its fully mature form–a self-synchronizing capability. So the performance and efficiency will be arising of edge structure of referral system. In the other hand, in this structure the request, referral and reply pattern of interactive will be arise the trust and trustworthy.

III. Trust, Delegation, Precommitment and Appearance

A virtual organization is a dynamic collection of entities (individuals, enterprises, and information resources) collaborating on some computational activity. Virtual organizations are an emerging means to model, enact, and manage large-scale computations. Virtual organizations consist of autonomous, heterogeneous members, often dynamic exhibiting complex behaviors. Thus, virtual organizations are best modeled via multiagent systems. An agent can be an individual such as a person, business partner, or a resource. An agent may also be a virtual organization. A virtual organization is an agent that comprises other agents. Collaborations among agents are structured via contracts. A contract is modeled as a set of commitments or precommitments. A virtual organization is formed between the contracting agents if it does not exist already. Virtual organizations can have complex nested structures and hence contracts may be formed at multiple levels. More than one contract may simultaneously exist among a set of contracting agents. Here, the virtual organizations within which the contracts are formed may overlap resulting in situations where an agent belongs to two or more virtual organizations, neither of which is an ancestor of the other.

We claim that trust is the mental counter-part of delegation, i.e. that it is a structured set of mental attitudes characterising the mind of a delegating agent/trustor, however obviously there are important differences, and some independence, between trust and delegation. Trust and delegation are not the same. The word "trust" is also ambiguous, it denotes both the simple evaluation of before relying on it (we will call this "core trust"), the same plus the decision of relying on y (we will call this part of the complex mental state of trust "reliance"), and the action of trusting, depending upon y (this meaning really overlaps with "delegation" and we will not use the term Delegation necessarily is an action, a result of a

decision, and it also creates and is a (social) relation among x, y, and The external, observable action/behavior of delegating either consists of the action of provoking the desired behavior, of convincing and negotiating, of charging and empowering, or just consists of the action of doing nothing (omission) waiting for and exploiting the behavior of the other. Indeed, will we use trust and reliance only to denote the mental state preparing and underlying delegation (trust will be both: the small nucleus and the whole). The strong delegation will be relation to action and precommitment. Strong delegation is based on y's awareness of x's intention to exploit his action; normally it is based on y's adopting x's goal (for any reason: love, reciprocation, common interest, etc.), possibly after some negotiation (request, offer, etc.) concluded by some agreement and social commitment. Therefore, if the trust and trustworthy of x to y will reinforce and strong then the precommitment as a y,s mental state will be made.

Appearance factor in trust concept is related to mental state. In fact, Trust basically is a mental state, a complex attitude of an agent towards another agent about the behavior and action that relevant for the result (goal). In referral social network, user agents have the main role. Every user in virtual organization has a user agent and every user agent will provide interfaces for correspondence user. By peer to peer communication of user agents in referral network, the trust and trustworthy will be diffuse and reinforce, and so the scope of every user agent and correspondence user will be extend. In fact, the appearance factor of trust mental state of correspondence users will be made and grew.

IV. Secrecy in Virtual Organization

The main purpose of information security systems is to defend against adverse impacts. Generally, the strength of a security system is determined by the weakest link. In many cases it is the human operator who represents the weakes link [16]. Social engineering attacks precisely target the human link, and represent a very effective attack vector. Security systems must be viewed as socio-technical systems that depend on the social context in which they are embedded to function correctly [14]. Security systems will only be able to provide the intended protection when people actually understand and are able to use them correctly. There is a very real difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly). In many cases, there is a trade-off between usability and theoretical security.

Poor usability of security systems and the consequences thereof have been pointed out by several authors. Whitten and Tygar's study [21, 22] on the usability of PGP is considered to be pioneering in this field. The importance of the usability aspect of security was discussed by earlier authors like Zurko and Simon [23], and even more than 100 years earlier by the Belgian cryptographer Auguste Kerckhoffs [9], who is most known for establishing the principle that security should not be based on obscurity. Below is the list of Kerckhoffs' security principles1 1) The system must be substantially, if not mathematically,undecipherable;2) The system must not require secrecy and can be stolen by the enemy without causing trouble; 3) It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants; 4) The system ought to be compatible with telegraph communication; 5) The system must be portable, and its use must not require more than one person; 6)Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules. Security principles 3 and 6 are in fact usability principles that are particularly relevant today, but that unfortunately have been mostly overlooked in the last 120 years [9].

Usability feature shows that the security systems is a essential concept of human interaction and so we need the mechanisms that the usability and so the security will be grew [12]. In the other hand, usability feature will be advanced the performance and contextual facilitation as “culture of trust".

All organizations keep secrets to protect themselves from exploitation by other organizations and to preserve the privacy of their agents [20]. But organizations that want to keep unnecessary secrets will also find this technology helpful, and this can hurt trust in regard to Sztompka's issues of appearance and accountability. The trust is a positive concept that provides the mechanisms for security process similar agent and service identify. In this perspective, appearance and accountability as two important factors of trust will be hold for agents and participants. This is a political issue, however, and agents may have different ideas than their organization does about what should be kept secret [18]. Organizations need to legitimize themselves, and secrecy erodes legitimacy. If taxpayers cannot see what their taxes are being spent on, or militaries fail to protect a country despite their secrecy, dissatisfaction grows.

Secrecy includes prevention of correlating disparate pieces of non-secret information to infer secrets. For instance, knowledge of the average salary of female employees in a department can be combined with knowledge there is only one female employee in the department to infer her salary. However, these problems are well known by statistical agencies, and automatic checks can be made before releasing correlatable information [1].

V. Reputation in Virtual Organization

The concept of reputation is closely linked to that of trustworthiness, but it is evident that there is a clear and important difference. We will define reputation is what is generally said or believed about a person’s or thing’s character or standing. In virtual organization, reputation is a quantity derived from the underlying social network which is globally visible to all members of the network, and so appearance factor will be reinforced. The trust and reputation

concepts are not equal, the trust maybe equal to good reputation in the special case and on the other case maybe yield for the bad reputation. The main differences between trust and reputation systems can be described as follows: Trust systems produce a score that reflects the relying party's subjective view of an entity's trustworthiness, whereas reputation systems produce an entity's (public) reputation score as seen by the whole community. Secondly, transitivity is an explicit component in trust systems, whereas reputation systems usually only take transitivity implicitly into account. Finally, trust systems usually take subjective and general measures of (reliability) trust as input, whereas information or ratings about specific (and objective) events, such as transactions, are used as input in reputation systems. Reputation can thus be seen as an asset, not only to promote oneself, but also as something that can be cashed in through a fraudulent transaction with high gain. It emerges that reputation systems have a multitude of complex facets, and is becoming a fertile ground for research.

Sztompka's issues of trust and reputation system are analogy in these factors:

1) the reputation factor 2)appearance is the main analogy factor. 3) if the trust of service or if the trustworthy of An user agent for referral and reply treats will be reinforced by reputation systems (evidences will be grew) then the performance factor is better. The performance factor will be calculated in the referral network in which the query, referral and reply pattern is the communication protocol. 4) when the reputation will be arise, the scope of neighborhood will be extended and the contextual facilitation factor as culture trust may be grow. 5) if the evidences of a service of a user agent will be grew the precommitment as a cognitive and sociality entity will be reinforced.

VI. Referral Policies in Virtual Organization as Referral Network

A referral policy specifies to whom to refer. We consider some important referral policies. In referral system, an agent answers a query only when it is sure of the answer. This ensures that only the providers answer any questions, and the consumers generate referrals to find the providers. 1. Refer all matching neighbors. The referring agent calculates how capable each neighbor will be in answering the given query (based on the neighbor's modeled expertise). Only neighbors scoring above a given capability threshold are referred 2. Refer all neighbors. Agents refer all of their neighbors. This is a special case of the matching policy with the capability threshold set to zero. This resembles Gnutella's search process where each servent forwards an incoming query to all of its neighbors if it doesn't already have the requested file. 3. Refer the best neighbor: Refer the best matching neighbor. This is similar to Freenet's routing of request messages, where each Freenet client forwards the request to a peer that it thinks is likeliest to have the requested information. The main result for the referral policies will be advanced the reputation, the appearance, the contextual facilitation factor as culture trust and the accountability of every user agent and the performance of different policies by varying the capability threshold.

VII. Authentication

Owners of systems and resources usually want to control who can access them. This is traditionally based on having a process for initial authorisation of identified parties, combined with operational mechanisms for authentication, and for controlling what resources those authenticated parties can access. There is thus a separation between authorisation, authentication and access control. The first common use of the term trust management was closely linked to the combination of authorisation, authentication and access control in distributed systems, as expressed by Blaze *et al* [7]. The main idea behind their approach was that a system does not need to know the identities of those who are accessing its resources, only that they are trusted to do so. This type of trust management is thus about verifying access credentials without necessarily authenticating entities. Blaze *et al.* defined trust

Authentication is an accountability technique related to auditing, and includes methods for verifying the integrity of information and the identity of people [16]. Authentication can confirm that virtual documents are unmodified, which is important since it is so easy to change them. Authentication can also prove that software (including auditing software) has not been tampered with, confirming that no viruses, worms, or other "Trojan horses" have been inserted. Authentication of virtual data uses methods of cryptography and "virtual signatures"; public-key cryptography is particularly useful because it can be used either to encrypt or to authenticate. Effective authentication methods prevent signatures from being copied from one document to another by making the signature a complicated function of the contents and date of the document. One of the important features of trust In referral system, will be achieved the accountability technique by answers of agent to a query only when it is sure of the answer. In fact, this mental state will be earned by referral policies and propagated and diffused by the referral or reply to any request.

Authentication can thus prove the author of a document, which prevents forgeries as well as later disavowal of authentic documents; this supports strong accountability. Authentication also can prove that a document in a sequence is missing, if one encrypts pointers to the previous and subsequent documents for each document. It can also identify sources of information leaks, by using steganography to embed unique hidden messages in each copy of a document, as in the pattern of spaces or line lengths [19].

In the case of referral networks, an agent would be considered authoritative if it has been pointed to by other authoritative agents. Recall that an agent is pointed to by other agents if it is providing useful answers or referrals. Hence, if an authority finds another agent useful and points at it, then it is reasonable that this agent be considered an authority as

well. That is, the agents decide on who is authoritative in the referral network. Hence in referral policy the authoritative agent will be gathered by the biggest value of intractives and so will be supported by user agent that every trustworthy of other user will be pointed to him.

VIII. Transactions and Feedback with Virtual Organization

Virtual organization should include more than making forms and reports accessible to agents; it should permit agents to affect organization processes [15], to address Sztompka's factors of performance and precommitment. Agents should be able to file applications for business permits online, for instance. Permitting such online transactions can simplify citizen's lives, reducing the amount of time they spend in organization offices and waiting in lines, and may be the only possible way to deliver services for widely scattered organizations and those of developing countries with limited infrastructures. Providing such services increases citizen trust that organization procedures are functioning appropriately. Online transactions can also eliminate much of the opportunity for bribes and other forms of corruption, and can remove some of the subjectivity of bureaucratic decision-making by implementing some decisions with computer algorithms. This provides more fairness [2].

Virtual organization also permits feedback from agents to the organization to give agents a better means to influence it. For instance, online surveys can assess citizen opinion, which is helpful even for nonrandom samples of agents or agents can actually vote online. Proposed or existing laws and regulations can be subjected to comments on discussion boards, giving the organization feedback about unanticipated problems, increasing the fairness of the laws and regulations and improving citizen trust in them. The referral policies make and arise the shared mental model of any user agents. And so shared ontology, common beliefs and knowledge, shared intention, shared structure, shared directives and shared plan may be result. The trust, trustworthy and the six Sztompka's factors are the main dynamic of this shared mental model.

IX. Conclusion

Virtual Organization as a social network and is contained the referral policies. The edge structure and referral policies have a trust core by six Sztompka's factors performance, reputation, appearance, accountability, precommitment, and contextual facilitation. We explain the feature of virtual organization in many perspectives. Virtual Organization can provide advantages for the agents: Easier access to important information, more reliable implementation of procedures, and better accounting for actions including assignment of responsibility. If virtual organization is implemented well by referral network, these benefits should increase the trust of agents in their organization because they increase the appearance of trustworthiness, consistency of performance, and accountability for actions. But agents are not very tolerant of incompetence in organization, and virtual organization must be implemented with carefully designed and carefully tested technology to gain these benefits.

References

[1] N. Adam and J. Worthmann, "Security-control methods for statistical databases: a comparative study", ACM Computing Surveys, 21 (4), 515-556, 1989.
[2] M. Bovens and Z. Stavros, "From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control". Public Administration Review, 62 (2), 174-184, 2002.
[3] K.M. Carley and M.J. Prietula, "Computational Organization Theory", Hillsdale, NJ, Lawrence Erlbaum Associates, 1994.
[4] P. Eckman, "Telling lies: clues to deceit in the marketplace, politics, and marriage", New York: Norton, 2001.
[5] I. Foster, C. Kesselman and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations", The International Journal of High Performance Computing Applications 15(3):200–222, 2001.
[6] B. Friedman, P. Kahn and D. Howe, "Trust online", Communications of the ACM, 43 (12), 34-40, 2000.
[7] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized trust management", In Proceedings of the 1996 IEEE Conference on Security and Privacy, Oakland, CA, 1996.
[8] D. Gambetta, " Can We Trust Trust?", in Trust: Making and Breaking Cooperative Relations, D. Gambetta, Ed. Basil Blackwell. Oxford, 1990, pp. 213.238.
[9] A. Kerckhoffs, "La cryptographie militaire. Journal des sciences militaries", IX(38):5.38 (January) and 161.191 (February), 1883. Available at F. Petitcola's Website: http://www.cl.cam.ac.uk/_fapp2/kerckhoffs/.
[10] N.Postman, "Technopoly: the surrender of culture to technology", New York: Vintage,1993.
[11] A.Jøsang and V.A.Bondi, "Legal Reasoning with Subjective Logic", Artificial Reasoning and Law, 8(4):289–315, winter 2000.
[12] S.Ross, "Security through Usability", Securius Newsletter,4(1), 2003.
[13] J.Prins, "E-organization and its implications for administrative law: regulatory initiatives in France, Germany, Norway, and the United States", London, UK: Cambridge, 2002.
[14] N.Rowe, "Designing good deceptions in defense of information systems", Computer Security Applications Conference, Tucson, AZ, 2004.
[15] R.Slayton and J.Arthur, "Public administration for a democratic society: Instilling public trust through greater collaboration with agents", In Malkia, M., Savolainen, R., and Anttiroiko, A.-V. (Eds.), E-transformation in governance: new directions for organization (pp. 110-130). Hershey, PA: Idea Group, 2003.
[16] R.Smith," Authentication: from passwords to public keys", Reading, MA: Addison-Wesley Professional, 2001.
[17] P.Sztompka, "Trust", Cambridge, UK: Cambridge University Press, 1999.
[18] A. Theoharis, "A culture of secrecy: the organization versus the people's right to know", Lawrence, KS: University Press of Kansas, 1998.
[19] P.Wayner, "Disappearing cryptography: information hiding: steganography and watermarking", San Francisco: Morgan Kaufmann, 2002.
[20] H.Yu, D.Kundur, and C.Y.Lin, " Spies, thieves, and lies: the battle for multimedia in the virtualera", IEEE Multimedia, 8 (3), 8-12, 2001.
[21] A. Whitten and J. Tygar, "Usability of Security: A Case Study", Computer Science Technical Report CMU-CS-98-155, Carnegie Mellon University, 1998.
[22] A. Whitten and J. Tygar, "Why Johnny Can't Encrypt:A Usability Evaluation of PGP 5.0.", In Proceedings of the 8th USENIX Security Symposium, Washington,D.C., August 1999.
[23] M. Zurko and R. Simon, "User-Centered Security", In C. Meadows, editor, Proc. of the 1996 New Security Paradigms Workshop. ACM, 1996.