

**A conceptualisation of a multidimensional model of trust and its antecedents for
knowledge sharing**

Abel Usoro

University of the West of Scotland, UK

abel.usoro@uws.ac.uk

Grzegorz Majewski

University of the West of Scotland, UK

grzegorz.majewski@uws.ac.uk

Matthew Kuofie

Central Michigan University, USA

kuofilm@cmich.edu

ABSTRACT

This paper conceptually develops a comprehensive model of trust that classifies antecedents of trust in information systems (IS) into (a) purely human-based, (b) purely IT-based, and (c) a combination of both. The research model is in the context of on-line knowledge sharing in virtual communities of practice (VCoP) which may involve various numbers of participants (from a few to a few thousands) and technologies. Implications of trust and its antecedents for IS/IT professionals are presented and discussed.

Keywords: *Information systems, knowledge sharing, virtual communities of practice*

1. INTRODUCTION

There have been research attempts to discover antecedents of trust in the use of information systems. Some research concentrate on technical factors (e.g. Kallath, 2005), others on human or organisational factors (e.g. Clarke, 2006) and yet others on a combination of both (e.g. Riegelsberger et. Al, 2003).

The combination of both technical and human factors is relatively new and therefore this paper aims to contribute to the current research effort towards developing a comprehensive trust model. This challenge is tackled by reviewing existing research to argue out a multidimensional model of trust. In the next step this model is related to on-line knowledge sharing in virtual communities of practice (VCoP). The model will in future be tested with an empirical study. Initial findings and implications are discussed and areas for future studies indicated. The rest of this paper is organised under (a) pure technology antecedents; (b) pure human antecedents; (c) technology as perceived by humans; (d) research model and hypotheses; (e) proposed methodology; and (f) conclusions.

2. PURE TECHNOLOGY ANTECEDENT

Trust is one of the most important factors affecting relationships between two or more people. In the modern world however this relationship does not have to be a direct, face-to-face, one. Technology allows such indirect relationships and works as an intermediary medium. It is also possible to relate participants' trust to the technology used. In this case trust may be perceived as "confidence in an entity to behave in an expected manner when

carrying out the intended purpose” (Kallath 2005, p. 4). Thus trust when used to technology itself becomes very similar to usefulness. Another related issue to trust when technology is so used is security. Trustworthiness in IT consists of four main aspects: integrity, non-repudiation, availability and authenticity (Kallath 2005, p. 4). It is expected that systems meet these requirements if they are to be trusted.

Trustworthiness should be assured across different components of the technology-enhanced communications such as medium, network, hardware and software. At each stage there are vulnerabilities that may be exploited that could damage the level of trust. The discipline that is addressing these problems is the trusted computing (TC) – a concept that originated from the Trusted Computing Group (TCG) which is a consortium of computer and device manufacturers, vendors and other parties who seek to improve communication security across multiple platforms and devices. Some of the most prominent members are Intel, HP, Microsoft, Sony and IBM. The TC concept is based on the new generation of hardware and software. One of the most interesting aspects of the concept is the addition of a tamper-resistant hardware chip, which could provide a basis of trust for all software run on the system. It also protects information on the system from potential software-based attacks and physical theft (Kallath 2005, p. 4). The way it facilitates the security and trust is the analysis of the user behaviour, encryption and other features.

Most communication nowadays is performed by using networks that are built on top of different media (e.g. copper, fibre, wireless) and this may be another trust concern. Building trust relationships based on security is “embedded” in various protocols and

regulations usually generated by the lengthy assurance processes, sometimes arranged and agreed off-line. They are expected to be valid on a long term basis and “certain at the time when trust relations derived from them are exercised” (Ren et. al. 2004, p. 687-688). In this notion trust is a derivative of the technology’s nature which itself at the same time is an antecedent of trust. It may get a little bit complicated in the case of *ad hoc* networks due to their “mobile” and “temporary” basis because of not always having the opportunity to agree on the connection protocols. Dynamic network topology may also complicate the trust and security situation. Thus it may be difficult to build trust-based relations in such an environment. Since it is expected that most networks will have such temporary or *ad hoc* characteristics, it is necessary to examine how to achieve trust in all networks. Some of the solutions proposed are the establishment of a Certificate Authority or Key Distribution Centre. These entities are responsible for “setting up the foremost trust relationships among all the nodes by distributing keys and certificates” (Ren et. al. 2004, p. 688). Another way to address these issues is the PGP¹-like distributed trust establishment scheme where the social relationships among nodes become the trust evidence for building trust itself (Hess et. Al 2005; Hubaux et. al. 2001). This approach is very important from the view of this work as it brings together the technology and human (social) perspectives in establishing trust relationships. This idea was further developed by Ren et. al. (2004) in the concept of chain of trust relationships (trust chain).

Trust may be achieved by a combination of a variety of hardware, software and network solutions. Such solutions may range from curtailed memory through attestation, sealed

¹ PGP stands for Pretty Good Privacy – a term invented by Philip Zimmermann in 1991 to describe a computer program that provides cryptographic privacy and authentication often with e-mail communications.

storage to protected input and output. In the case of the curtailed memory there are only small parts of the software that can run with extra privileges. At this step it is necessary to remember that the existing widely used operating systems do not usually provide adequate mechanisms that separate programs from one another. Thus if only one part gets an extra privileges (to for example have access to the encryption features) it is possible to say that the level of trust has increased. On the software side this module with extra privileges can be accessed via interfaces by other applications for the benefit of the user. Attestation may be used to assess the integrity of the information itself. It is used to assure that software or the information has not been changed in some unintended manner. Protected input and output and sealed storage are the measures taken on the hardware side to enable the encryption of the information and the communication between applications and devices such as keyboard, mouse or monitor (Kallath 2005, p. 5).

Apart from the medium, network, hardware and software trust may be affected by the complexity and transparency of the technology utilized to facilitate it. The environment that is transparent to the user is in turn more trusted. Transparency is believed to “facilitate compliance, effectiveness and the ability to assess both” (Weber 2008, p. 344). Akkermans et. al. (2004) stress the importance of transparency in regards to data and knowledge. Their research also shows the link between the technological transparency and the level of trust. Transparent systems and technology are also easier for use (thus the general notion of usability and trust is achieved) as indicated by Dinka et. al. (2006). On the other hand the complexity of the system may affect the trust level both in a negative and in a positive way. It is expected that more complex systems facilitate security and

usability better; while on the other hand they may decrease the transparency level and be difficult to learn (i.e. usefulness may be decreased at the early stage). Trust plays also a major role in newest approaches like cloud and grid computing (Luo, J. et. al. 2009).

The foregoing discussed factors constitute the technological antecedents of trust based relations. As technology is usually associated with the humans that use it, in the next paragraphs we will discuss the pure human antecedents of trust.

3. PURE HUMAN ANTECEDENTS

Apart from the technology utilized for the purposes of communication, trust in on-line environment may also be perceived at a human level. If someone does not trust a person in real life why should he or she trust him or her in the “virtual life”? In human relations, trust may be perceived as a “willingness to be vulnerable based on positive expectations about the actions of others” (Riegelsberger et. al. 2003, p 761). This definition is an abstract one as it does not define any sources of vulnerability, or structure of trust requiring situations. For the purposes of this research and future empirical research it is necessary to use an extended definition of trust as provided by Gambetta:

“Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both *before* he can monitor such action (or independently of his capacity ever to be able to monitor it) *and* in a context in which it affects *his own* action” (Gambetta, 1990, p. 218).

This definition distinguishes two roles a person can play in the trust-based relationship: the *trustor* role of allowing oneself to be vulnerable to actions performed by others and trusting their actions; and the *trustee* role of performing actual actions and deciding whether to cooperate or no. This definition is concerned with asynchronous trust, which is a common situation for most of the on-line communication where communication is also

asynchronous. It also implicitly introduces the concept of trustworthiness. It does not say however what the sources of vulnerability are.

The sources of vulnerability in real life situations are based on whether the trustee is skilled enough to perform a given action required by the trustor (competence), whether his or her intentions are correct and does not want to cheat the trustor (integrity) and whether he or she actually wants to perform the action required by the trustor (benevolence). Thus trust may be perceived as a phenomenon relating to each of the sources of vulnerabilities. However usually the trustor does not know the characteristics of the trustee in depth and bases his or her trust rather on perceived values of competence, integrity and benevolence. These attributes of another party (trustee) were identified by Mayer et. al. (1995) and mapped to on-line knowledge sharing situation in virtual communities of practice by Usoro et. al. (2007). Trust may be perceived as an antecedent to a variety of on-line activities (e.g. e-commerce and knowledge sharing). Usoro et. al. constructed a conceptual model of trust as an antecedent of on-line knowledge sharing and tested it empirically with a global corporation. This empirical study is very interesting and relevant to this research as it indicates that these dimensions of trust are significant.

Trust in an on-line environment may be perceived as a psychological and social phenomenon. It is thus necessary to take into account factors from these two domains as they may influence the decisions of participants. Victor et al. (2009) argue that “collaboration, and information sharing are the main driving forces of the new generation of web applications referred to as ‘Web 2.0’ such as weblogs, wikis and social networks”

while trust may enhance the user experience of such application (Victor et al. 2009, p. 1367-1369). Previously mentioned perceived competence, integrity and benevolence may influence both individual and group decisions; thus they are relevant both to psychological and social perspective. Walczuch & Lundgren (2004) group the psychology related trust antecedents into five groups:

- Personality-based
- Perception-based
- Experience-based
- Knowledge-based
- Attitude

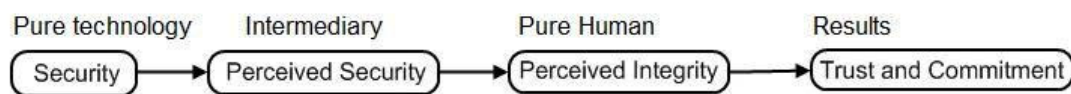
Personality-based trust antecedents relate to such factors as extraversion, openness to experience, propensity to trust, agreeableness, neuroticism and conscientiousness. Some of them influence trust positively while others are in a negative way. Perception-based trust antecedents embrace perceived reputation (word-of-mouth, marketing data and other sources), perceived-control and perceived familiarity. Experience-based is concerned with experience over time and such factors as satisfaction and communication. Knowledge-based antecedents of trust refer to the perceived information and data security, while attitude is concerned with the IT literacy and a general willingness to “do something on-line”.

Social antecedents of trust are concerned with the features of groups of people instead of individuals. Within these antecedents, it is possible to identify such factors as culture to which participants belong (Riegelsberger et. al. 2003; Usoro & Kuofie 2006), strengths of the ties within the social network (Marouf 2007), social network itself, social trust and shared goals (Chow & Chan 2008).

4. TECHNOLOGY AS PERCIEVED BY HUMANS

Interactions between humans with the use of ICT are not physical but mediated. Trust in such interactions is influenced not by the real actions of the other party but rather by what is visible on the other end of the communication channel. Moreover it is not only the actual knowledge of the underlying technology that is important but rather the way it is perceived by the users. Thus it is necessary to introduce a new layer between the pure technology and pure human-related factors affecting trust. The new layer contains the intermediary antecedents of trust - factors that are mirroring the perceived usefulness of the communication technology. Figure 1 presents a simplified example of how these layers match each other:

Figure 1. Trust antecedents matching



In this perspective trust appears to be a multidimensional phenomenon stretching through pure technology, technology as perceived by users with their individual. Reliable trust and commitment are based on the underlying antecedents. Intermediary antecedents of trust embrace a wide spectrum of factors such as

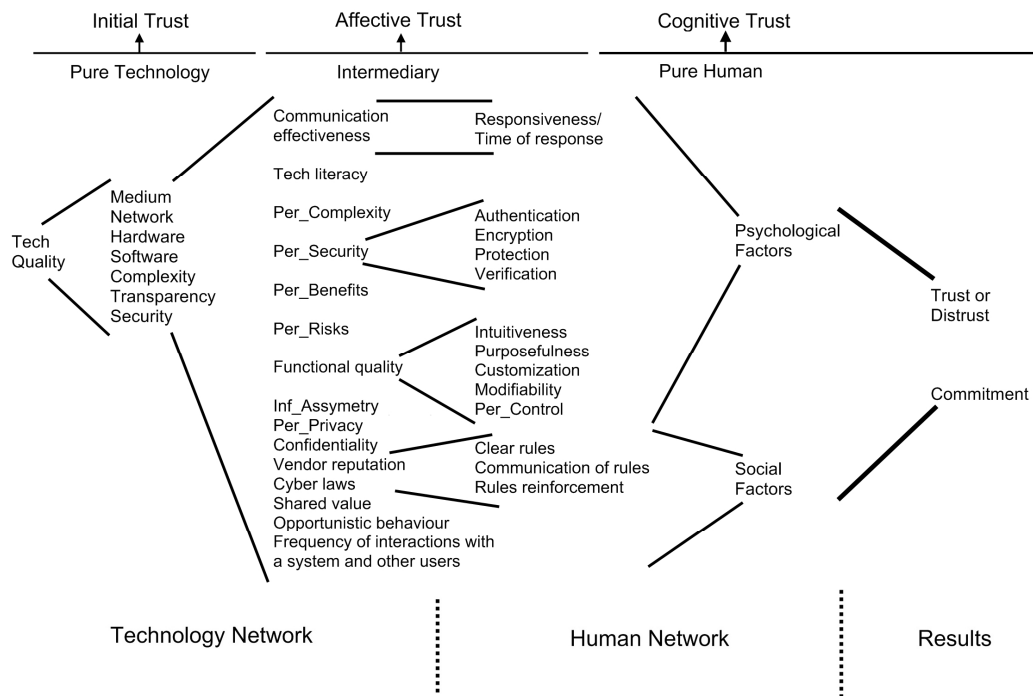
communication effectiveness (Sharma & Patterson 1999, Mukherjee & Nath 2003, Riegelsberger et. al. 2003, Arnott 2007), perceived complexity (Mukherjee & Nath 2003), perceived security (Ramnath & Pavlou 2002, Mukherjee & Nath 2003, Lenzini et. al. 2008), responsiveness (Mukherjee & Nath 2003), perceived benefits (Riegelsberger et. al. 2003, Li et al. 2008) and perceived risks (Mukherjee & Nath 2003, Riegelsberger et. al. 2003, Li et al. 2008, Sarlak & Hastiani 2008). See Appendix I for a comprehensive list of trust antecedents with relation to results: trust and commitment.

5. RESEARCH MODEL AND HYPOTHESIS

The multidimensional model proposed by this work encompasses the three layers of trust in web based interactions and the expected results, which are trust and commitment. Moreover we tried to relate the model to the concepts of initial trust as well as affective trust and cognitive trust. Li et al. (2008) investigates the concept of initial trust and how it affects the adoption of IS. He notes that “the decision to readily adopt a new technology is influenced by users’ initial perception of the technology” (idem. p. 40). This situation may occur when users know something about the IS in advance (word-of-mouth, experiences with similar systems or prototype). This perspective on early adoption of IS aligns with the research on initial trust. It is true that trust is a phenomenon that develops over time; however in the case of a novel technology it may be very important not to underestimate the initial level of trust – a starting point for a yet-to-come trust. In the multidimensional model of antecedents of trust proposed by this work initial trust is related to the first layer (technology network) of the users’ experience. It is expected that more sophisticated forms of trust (affective and cognitive) will develop with time while the users gain more opportunities to interact with the system and each other.

McAllister (1995) distinguished between affective trust (which is based on underlying feelings) and cognitive trust (which is based on reasoning). Affective trust is more temporary and concerned with the current situation which is to some point affected by some interaction with technology. For example a system may be responding particularly slowly on a given day and this may have impact on the frustration and trust levels of the users. However provided that this situation does not repeat very often users may still trust each other and the communication technology. Affective trust can thus be influenced by experience with technology whereas cognitive trust may not be directly affected since it works on a different principle. Cognitive trust works on the principle of reasoning as performed by the users about the technology and their co-users. Technology and communication itself is not directly involved but rather it is more of a process inside the brains of the users. This level of trust is thus much more related to pure human antecedents of trust. Figure 2 presents the multidimensional model of trust.

Figure 2. Multidimensional model of trust

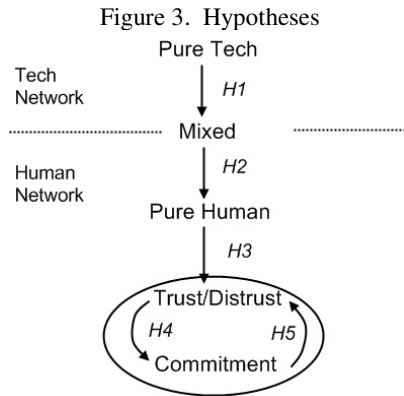


(Note: “Per” stands for “Perceived” as in “Per_Complexity” referring to “Perceived Complexity”.)

Based on the model presented we have formulated a set of hypotheses which are aimed at testing the validity of the model:

- H1: Pure Technological factors affect Intermediary Factors (e.g. Security affects perceived security)
- H2: Intermediary Factors affect Pure Human factors
- H3: Pure human factors affect the level of Trust/Distrust
- H4: Trust affects Commitment
- H5: Commitment affects Trust

The flow of the hypotheses is presented on figure 3 below:



6. PROPOSED METHODOLOGY

In order to evaluate the validity of the multidimensional conceptual model we would like to apply a combination of qualitative and quantitative techniques. We believe that such approach is the most effective given the complexity of the phenomenon researched and the fact that the human perceptions and beliefs play a significant role. This approach has also been employed by Mohammad & Hastiani (2008) to assess the validity of their model of trust in virtual universities. In the first phase we would like to identify what the most important factors affecting the knowledge sharing behaviour of participants of a given virtual community of practice are and whether they are similar to the factors mentioned previously. This would be the qualitative part of the research in the form of interviews with key members of a VCoP (the manager and a few members). In the next step a quantitative approach would be used to assess whether these factors are valid across majority of the members.

7. CONCLUSION

The concept of trust is very important for a variety of on-line activities and environments. Web based communities and knowledge sharing in VCoP in particular are some of the most common examples. Trust is however not a simple phenomenon but rather a very complex one with a great number of uncertainties. This study proposed a multidimensional model of trust and related it to on-line knowledge sharing. In order to embrace the most critical factors of trust and commitment it is sometimes necessary to “go back” from (a) purely human perspective through (b) how users perceive the underlying technology to (c) the technology itself. In some cases it is unknown what could go wrong and there is a necessity to have a wider picture. We hope this paper provides such a broad perspective. This broad perspective will be validated in a future empirical research.

Appendix I

No	Perspective	Factor	Article
1	Technology	Medium	Kallath (2005)
2	Technology	Network	Ren et. al. (2004), Kallath (2005), Li et al. (2008)
3	Technology	Hardware	Kallath (2005), Li et al. (2008)
4	Technology	Software	Kallath (2005), Li et al. (2008)
5	Technology	Complexity	Akkermans et. al.(2004), Kallath (2005), Li et al. (2008)
6	Technology	Transparency	Akkermans et. al.(2004), Dinka et. al. (2006), Weber (2008)
7	Technology	Security	Mukherjee & Nath (2003), Lenzini et. al. (2008)
8	Intermediary	Communication effectiveness	Sharma & Patterson (1999), Mukherjee & Nath (2003), Riegelsberger et. al. (2003), Arnott (2007)
9	Intermediary	Responsiveness/Time of Response	Mukherjee & Nath (2003)
10	Intermediary	Technology literacy	Mukherjee & Nath (2003)
11	Intermediary	Perceived Complexity	Li et al. (2008)
12	Intermediary	Perceived Security (e.g. Auth)	Ramnath & Pavlou (2002), Mukherjee & Nath (2003), Lenzini et. al. (2008),
13	Intermediary	Perceived Benefits	Riegelsberger et. al. (2003), Li et al. (2008)
14	Intermediary	Expectations	Li et al. (2008),
15	Intermediary	Satisfaction	Hess & Story (2005), Li et al. (2008)
16	Intermediary	Perceived Risks	Mukherjee & Nath (2003), Riegelsberger et. al. (2003), Li et al. (2008), Sarlak & Hastiani (2008)
17	Intermediary	Functional Quality	Kallath (2005)
18	Intermediary	Personalisation	Mukherjee & Nath (2003)
19	Intermediary	Perceived Control	Clarke, N. (2006)
20	Intermediary	Information Asymmetry	Mukherjee & Nath (2003)
21	Intermediary	Perceived privacy	Mukherjee & Nath (2003)
22	Intermediary	Confidentiality	Mukherjee & Nath (2003)
23	Intermediary	Reputation (also vendor reputation)	Mukherjee & Nath (2003), Sichtmann (2007), Li et al. (2008), Sarlak & Hastiani (2008)
24	Intermediary	Cyber Laws (also reinforcement)	Mukherjee & Nath (2003)
25	Intermediary	Regulatory Control	Mukherjee & Nath (2003)
26	Intermediary	Perception of technological competency	Mukherjee & Nath (2003)

27	Intermediary	Shared value	Mukherjee & Nath (2003), Clarke, N. (2006)
28	Intermediary	Opportunistic behaviour	Mukherjee & Nath (2003)
29	Intermediary	Frequency of interactions with a system and other users	Riegelsberger et. al. (2003)
30	Intermediary	Change (e.g. software updates)	Li et al. (2008)
31	Human	Psychological factors (personality, stress, pressure)	Riegelsberger et. al. (2003), Walczuch & Lundgren (2004), Sarlak & Hastiani (2008)
32	Human	Social factors	Riegelsberger et. al. (2003), Gefen, D., Straub, D. W., (2004), Arnott (2007), Marouf (2007), Chow & Chan (2008), Sarlak & Hastiani (2008)
33	Human	Perceived Integrity	Riegelsberger et. al. (2003), Smith, G. (2005), Arnott (2007), Usoro et. al. (2007) Sarlak & Hastiani (2008)
34	Human	Perceived Competence	Arnott (2007), Usoro et. al. (2007), Sarlak & Hastiani (2008)
35	Human	Perceived Benevolence	Riegelsberger et. al. (2003), Arnott (2007), Usoro et. al. (2007)
36	Human	Culture	Riegelsberger et. al. (2003)
37	Human	Motivation	Riegelsberger et. al. (2003)
38	Human	Direct/Indirect experience	Arnott (2007), Li, X et al. (2008)
39	Organization	Policy	Smith, G. (2005), Clarke, N. (2006), Li et al. (2008), Mun, J. et. al (2009)
40	Organization	Type (Profit or non-profit)	Smith, G. (2005), Li et al. (2008), Sarlak & Hastiani (2008)
41	Organization	Regulations	Clarke, N. (2006)
42	Organization	Size	Sarlak & Hastiani (2008)
43	Results	Trust/Distrust	Mukherjee & Nath (2003), Riegelsberger et. al. (2003), Hess & Story (2005), Clarke, N. (2006), Arnott (2007), Usoro et. al. (2007), Li et al. (2008) (initial trust)
44	Results	Commitment	Mukherjee & Nath (2003), Hess & Story (2005), Clarke, N. (2006), Usoro et. al. (2007)
45	Results	Measurement	Riegelsberger et. al. (2003), Hess & Story (2005), Li, X et al. (2008)

REFERENCES

- Akkermans, H., Bogerd, P. & van Doremalen, J., (2004), Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics, *European Journal of Operational Research*, Vol. 153, pp. 445-456.
- Arnott, D. C., (2007), Trust – current thinking and future research, *European Journal of Marketing*, Vol. 41, No. 9/10, pp. 981-987.
- Chow, W. S. & Chan, L. S., (2008), Social network, social trust and shared goals in organizational knowledge sharing, *Information & Management*, 45, pp 458-465.
- Clarke, N. (2006), The relationship between network commitment, its antecedents and network performance, *Management Decision*, Vol. 44, No. 9, pp. 1183-1205.
- Dinka, D., Nyce, J. M., Timpka, T., (2006), The need for transparency and rationale in automated systems, *Interacting with Computers*, Vol. 18, pp. 1070-1083.
- Eschenaure, L., Gligor, V. D. & Baras, J., (2002), On trust establishment in mobile ad-hoc networks, *Proceedings of the Security Protocols Workshops*, Cambridge, 2002.
- Gambetta, D., (2000) Can We Trust Trust?, in Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp 213-237.
- Gefen, D., Straub, D. W., (2004), Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services, *Omega*, 32, pp. 407-424.
- Hess, J. & Story, J., (2005), Trust-based commitment: multidimensional consumer-brand relationships, *Journal of Consumer Marketing*, 22/6, pp. 313-322.

- Hubaux, J., Buttyan, L., Capkun, S., (2001), The quest for security in mobile ad hoc networks, Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, CA, USA, 2001.
- Kallath, D., (2005), Trust in Trusted Computing – the end of security as we know it, Computer Fraud & Security, pp. 4- 7.
- Lenzini, G., Bargh, M. S. & Hulsebosch, B., (2008), Trust-enhances Security in Location-based Adaptive Authentication, Electronic Notes in Theoretical Computer Science, 197, pp. 105-119.
- Li, X., Hess, T. J. & Valacich, J. S., (2008), Why do we trust new technology? A study of initial trust formation with organizational information systems, Journal of Strategic Information Systems, 17, pp. 39-71.
- Luo, J., Ni, Xudong. & Yong, J. (2009), A trust degree based access control in grid environments, Information Sciences, XXX, pp 1 - 11
- Marouf, L. N., (2007) Social networks and knowledge sharing in organizations: a case study, Journal of Knowledge Management, Vol. 11, No. 6, 110-125.
- Mayer, R. C., Davis, J. H. & Schoorman, F. D., (1995), An integrative model of organisational trust, Academy of Management Review, 20(3), pp 709-734.
- McAllister, D. J., (1995), Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations, Academy of Management Journal, Vol. 38, No. 1, pp 24-59.
- Mohammad, A. S. & Hastiani, A. A., (2008), Trust in Virtual Universities, Journal of Social Sciences, 4 (3), pp 237-245.

- Mukherjee, A. & Nath, P., (2003), A model of trust in online relationship banking, *International Journal of Bank Marketing*, 21/2, pp. 5-15.
- Mun, J., Shin M., Lee, K. & Jung, M., (2009), Manufacturing enterprise collaboration based on goal oriented fuzzy trust evaluation model in a virtual enterprise, *Computers & Industrial Engineering*, 56, pp 888-901.
- Ramnath, K. C. & Pavlou, P. A., (2002), Perceived information security, financial liability and consumer trust in electronic commerce transactions, *Logistics Information Management*, Volume 15, Number 5/6 pp. 358-368.
- Ren, K., Li, T., Wan, Z., Bao, F., Deng, R. H. & Kim, K., (2004), Highly reliable trust establishment scheme in ad hoc networks, *Computer Networks*, 45, pp. 687-699.
- Riegelsberger, J., Sasse, M. A. & McCarthy J. D., (2003) The researcher's dilemma: evaluating trust in computer-mediated communication, *Int. J. Human-Computer Studies*, 58, pp. 759-781.
- Sarlak, M., A. & Hastiani, A. A., (2008), Trust in Virtual Universities, *Journal of Social Sciences*, 4(3), pp. 237-245.
- Sharma, N. & Patterson, P. G., (1999) The impact of communication effectiveness and service quality on relationship commitment in consumer, professional services, *The Journal of Services Marketing*, Vol. 13, No. 2, pp. 151-170.
- Sichtmann, C. (2007), An analysis of antecedents and consequences of trust in a corporate brand, *European Journal of Marketing*, Vol. 41, No. 9/10, pp. 999-1015.
- Smith, G. (2005), How to achieve organizational trust within an accounting department, *Managerial Auditing Journal*, Vol. 20, No. 5, pp. 520-523.

Usoro, A., & Kuofie, M. H. S., (2006) Conceptualisation of Cultural Dimensions as a Major Influence on Knowledge-Sharing, *International Journal of Knowledge Management*, Vol 2, Issue 1, August, pp 16 - 25.

Usoro, A., Sharratt, M. W., Tsui, E. & Shekhar, S., (2007) Trust as an antecedent to knowledge sharing in virtual communities of practice, *Knowledge Management Research & Practice*, Vol. 5, pp 199-212.

Victor, P., Cornelis, C., DeCock, M. & Silva, P. P., (2009), Gradual trust and distrust in recommender systems, *Fuzzy Sets and Systems*, 160, pp 1367-1382.

Walczuch, R. & Lundgren, H., (2004), Psychological antecedents of institution-based consumer trust in e-retailing, *Information & Management*, 42, pp 159-177.

Weber, R. H. (2008), Transparency and the governance of the Internet, *Computer Law & Security Report*, 24, pp. 342-348.