Context and Time Based Riskiness Assessment for Decision Making

Omar Khadeer Hussain [1], Elizabeth Chang [1], Farookh Khadeer Hussain [1], Tharam S. Dillon [2] and Ben Soh [3]
[1] School of Information Systems, Curtin University of Technology, Perth, Australia
{Omar.Hussain, Elizabeth.Chang, Farookh.Hussain}@cbs.curtin.edu.au
[2] Faculty of Information Technology, University of Technology, Sydney, Australia
tharam@it.uts.edu.au
[3] Dept of Computer Science and Computer Engineering, La Trobe University, VIC, Australia
ben@cs.latrobe.edu.au

Abstract

In an e-commerce interaction carried out in a Peer-to-Peer environment it is rational for the trusting peer to analyze the Risk that could be involved in dealing with a trusted peer as there is a lack of central management in these type of interactions. Risk analysis can be done by assimilating recommendations from other peers if there is no previous interaction history between the trusting peer and the trusted peer. But the assimilated recommendations might be according to the criteria of the recommending peer with the trusted peer, and it is not necessary for the trusting peer to have the same criteria in its interaction with the trusted peer as that of the recommending peer even thought it is interacting in the same context. Further it might interact in a different time as that of the recommending peer. The Risk that was present in a particular context and at a particular time might not be the same at a different time. Hence in this paper we discuss the process of the trusting peer assimilating the recommendations from the recommending peers according to the context, criteria and time of its interaction in order to determine the Riskiness value of the trusted peer, which would help it considerably in decision making.

1. Introduction

The process of conducting e-commerce transactions has revolutionalized with the advent and development of Internet [1]. It currently provides the user with numerous facilities which facilitate the transaction process. The two types of architectures through which e-commerce transactions can be conducted are:

a) Client-Server Business Architecture, and
b) Peer-to-Peer Business Architecture.

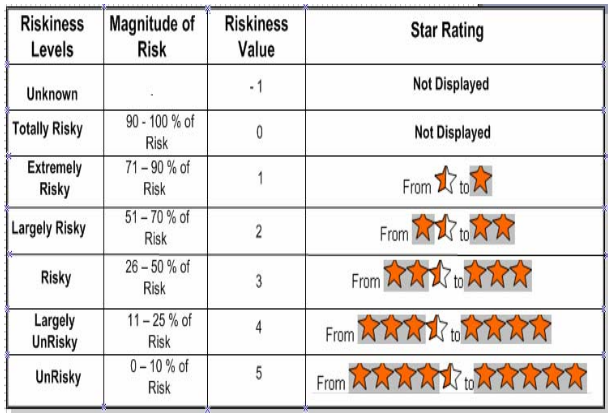
In Client-Server architecture, servers are powerful computers that specifically manage clients and network traffic [2]. In a Peer-to-Peer architecture each node has equivalent responsibilities [3]. This is a type of network in which each workstation or Peer has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers or central servers are dedicated to serving the others. The main difference between these two architectures is that in Peer-to-Peer architecture the control is transferred back to the clients from the servers, and it is the responsibility of the clients to complete the transaction [4]. Some of the characteristics of Peer-to-Peer or decentralized transactions are:

- There is no server in this transaction between Peers.
- Peers interact with each other directly, and the interactions are passed to them, rather than through a server as compared to a centralized transaction.
- Peers can forge or create multiple identities in a decentralized transaction, and there is no way of checking the identity claimed by the Peer to be genuine or not. On the other hand, in a centralized transaction it can be checked, as the information about the Peers is stored in the server.

From the above properties it can be concluded that a decentralized transaction carries more Risks and hence merits more detailed investigations. Decentralized transactions or Peer-to-Peer transactions can be compared with distance transactions that have much in common with catalogue mail ordering systems [3]. Distance transactions often provide insufficient information about the goods and service offered, and requires the consumers to accept the Risk of prior performance, which often leaves them in a vulnerable position. Hence there is a high level of Risk involved in decentralized transactions according to the consumer's point of view. Risk is important in the study of behavior in e-commerce, because there is a whole body of literature based in rational economics that argues that the decision to buy is based on the Risk-adjusted cost-benefit analysis [5]. Thus it commands a central role in any discussion of e-commerce that is related to a transaction. The need to distinguish between the likelihood and magnitude of Risk is important. This can be explained by taking the empirical evidence in a web based sale. For example the likelihood of selling an item on the web decreases as the cost of the product increases. For higher cost items, the web does not tend to act as a medium to buy, but as a means for providing information and vice versa for lower cost items. The likelihood of a negative outcome might be the same in both transactions, but the magnitude of loss will be greater in a higher cost transaction. Therefore, the relative reluctance of the customers to buy high cost items on the Internet, compared to the demand for lower cost items, would be consistent with the idea that magnitude of potential loss defines perception of Risk, and not likelihood of loss [6]. Risk plays a central role in deciding whether to proceed with a transaction or not. It can broadly be defined as an attribute of decision making that reflects the variance of its possible outcomes. Peer-to-Peer communications are being described as the next generation of the Internet [7]. Some researchers are proposing architectures for integrating web services with Peer-to-Peer communication agents like Gnutella [8-11]. However, Peer-to-Peer communications suffer from some disadvantages and Risk in the transaction is one of them. Risk analysis in the transaction is really important with the widespread use of the Internet, particularly with the advent of business and e-commerce transactions and the integration of Peer-to-Peer communications with web services [12]. Hence we need to develop a mechanism by which we can over come this disadvantage so that they can be used effectively with what ever service they is being integrated with.

2. Analyzing Risk by determining Reputation

In order to analyze the Risk that could be present in the interaction we defined the term Riskiness in Hussain et al [13]. Riskiness is defined as the numerical value that is assigned to the trusted peer by the trusting peer after its interaction with it. The Riskiness value shows the level of Risk that was present in the interaction on the Riskiness scale. The Riskiness scale as shown in Figure 1 has 7 different levels of Risk that could be present in the interaction. The semantics of the Riskiness scale are defined in Hussain et al [13]. The Riskiness value to a trusted peer is assigned by the trusting peer after assessing the level of un-commitment in the actual behavior of the interaction as compared to the promised commitment. The promised commitment is the expected behavior by which the trusted peer was supposed to behave in the interaction. This expected behavior is defined by the trusting peer before starting the interaction according to the criteria of its interaction. The actual behavior is the actual commitment that the trusted peer showed or behaved in the interaction. But the Riskiness value is assigned to the trusted peer by the trusting peer after its interaction with it. As mentioned in section 1 the decision to proceed in the transaction is based on the Risk adjusted cost benefit analysis. Hence it would be much easier for the trusting peer to decide whether to proceed or not in an interaction with a trusted peer, if it knows beforehand the level of Risk that could be present in interacting with it



Riskiness Levels	Magnitude of Risk	Riskiness Value	Star Rating
Unknown	-	- 1	Not Displayed
Totally Risky	90 - 100 % of Risk	0	Not Displayed
Extremely Risky	71 – 90 % of Risk	1	From ⯪ to ★
Largely Risky	51 – 70 % of Risk	2	From ★⯪ to ★★
Risky	26 – 50 % of Risk	3	From ★★⯪ to ★★★
Largely UnRisky	11 – 25 % of Risk	4	From ★★★⯪ to ★★★★
UnRisky	0 – 10 % of Risk	5	From ★★★★⯪ to ★★★★★

Figure 1 showing the Riskiness scale

It is possible that before starting an interaction, the trusting peer might have to choose from a set of possible trusted peers with whom to interact with in a given context. If the trusting peer has not interacted with any of the possible trusted peers in the particular context of the interaction, then it doesn't know the level of Risk that could be involved in dealing with any particular trusted peer and hence it is difficult for it to conclude and decide, with which trusted peer to interact with. An indication of Risk that could be present in dealing with a particular trusted peer before starting the interaction can be achieved by asking for recommendations or its reputation from other peers. Reputation can be used as an alternative in decision making when the Riskiness of the trusted peer is not known [17]. The higher the reputation of a particular peer the lower the Risk that could be present in interacting with it. After getting the recommendations or reputation about a particular trusted peer from other peers, the trusting peer can assimilate them according to the criteria of its interaction and then determine the Riskiness value of the trusted peer on the Riskiness scale. Once the trusting peer gets the Riskiness value of all the trusted peers then it can decide with which particular peer to interact with.

Reputation about a particular trusted peer can be considered from peers who have interacted with it before. The trusting peer issues a reputation query asking for recommendations about a trusted peer specifying the context of its interaction. It gets recommendations from peers who had interacted with the particular trusted peer previously in the same context. The peers giving recommendations are called as the Recommending peers [15]. The recommending peers reply back with the Riskiness value that they assigned to the trusted peer in their interaction with it as their recommendation to the trusting peer in the form of a Risk set. The Risk set is an ordered way of soliciting recommendations by the recommending peers, so that it is easier for the trusting peers to interpret it. The format of the Risk set is discussed in Hussain et al [14]. The Risk set contains the recommended Riskiness value which the recommending peer recommends for the trusted peer. The trusting peer can then assimilate the recommendations and determine the Riskiness value of the trusted peer, which would help it in deciding whether to interact with the trusted peer or not.

2.1 Context and Assessment Criteria of the Recommendations

As mentioned earlier, the recommending peers reply back with the Riskiness value that they assigned to the trusted peer as their recommendation. But the Riskiness value that the recommending peer recommends is according to the assessment criteria of its interaction. Assessment criteria are the factors or bases against which the un-committed behavior of the trusted peer was assessed by the recommending peer.

In this paper we will term the assessment criteria as criteria. It is possible that a trusting peer asking for recommendations for a trusted peer in a particular context might have the criteria in its interaction different as compared to other trusting peers who had interacted previously with the same trusted peer, in the same context. Subsequently the Riskiness value which each trusting peer assigns to the trusted peer after the interaction is according to the criteria of its interaction. Hence even in the same context, two trusting peers 'A' and 'B' might have different criteria in their interaction with the same trusted peer 'C', and the Riskiness value they assign to the trusted peer 'C' is according to the criteria of their interaction. If at a later stage when any other trusting peer asks for recommendations about trusted peer 'C' from peers 'A' and 'B' in the same context as their interaction, then they reply back with the Riskiness value that they assigned to the trusted peer 'C' as their recommendation. But the Riskiness value recommended by the recommending peers 'A' and 'B' for the trusted peer 'C' is based on the criteria of their interaction. It is extremely possible that the recommendation might not be of any use to the trusting peer as it might have a different set of criteria in its interaction as compared to the recommending peers even though it is in the same context. Hence the trusting peer while assimilating the recommendations should take only those recommendations whose assessment criteria are of interest to it. Also while assimilating the recommendations; it is important for the trusting peer to consider the time at which the recommending peer interacted with the trusted peer. As discussed in Hussain et al [15] Risk is dynamic and keeps on changing according to time. When the trusting peer is considering the recommendations then it should give more weight to recent interactions of the trusted peer with any other recommending peer as compared to the far recent ones. Another important factor for the trusting peer to consider while assimilating the recommendations is to determine whether the recommending peer is giving trustworthy recommendation or not. It is possible that a recommending peer might be giving un-trustworthy recommendations too. The trusting peer has to consider all these scenarios before it assimilates the recommendations and determines the Riskiness value of a trusted peer. We have discussed the process of classifying the recommendations as trustworthy or untrustworthy in Hussain et al [18]. To summarize a peer whose Riskiness value while giving recommendation (RRV) is in the range of (-1, 1) is said to be giving trustworthy recommendations. Further in this paper we will refer to the criterions in the interaction as C_1, C_2 …C_n, where n represents the number of criterions in the interaction.

2.2 Time Based Riskiness Assessment

We define Risk as the likelihood that the trusted peer will not act as expected by the trusting peer resulting in the loss of resources involved in the transaction [16]. This 'likelihood' varies throughout the transaction depending on the behavior of the trusted peer and hence it is dynamic. Some of the possible scenarios of the variance in the likelihood are:

- The trusting peer's expectations are not being met by the behavior of the trusted peer.
- The recommendations that the trusting peer gets from the other peers might either strengthen or lessen its belief that it has for the trusted peer over a period of time, and hence varying the likelihood of loss too.

Hence the trusting peer should give more weight or importance to the recommendations from the recommending peers who had interacted with the trusted peer recently as compared to the far recent transactions. We will define some terms which are necessary for classifying the recommendations according to time.

We term the reputation of a peer at a given context and at a given time't' which can be either at the current, past or future time as its *Riskiness value*.

We define the total boundary of time which the trusting peer is taking into consideration to assess the Riskiness value of a trusted peer as the *time space*.

But it is not possible for the trusting peer to assess the behavior of the trusted peer correctly if the time space is of a long duration. As mentioned earlier, Risk varies according to time and it is possible that in a time space the trusted peer's Riskiness value might not be the same throughout. Hence the total time space is divided into different non-overlapping parts and the trusting peer assess the Riskiness value of the trusted peers in each of those parts. These different non-overlapping parts are called as *time slots*.

The time at which the trusting peer or any other peer giving recommendation dealt with the trusted peer in the time slot is called as *time spot*.

For explanation sake let us suppose that the trusting peer wants to assess the behavior of the trusted peer for over a period of 28 days, and wants to analyze the behavior on a weekly basis. Hence the total *time space* is 28 days and the *time slot* is of 7 days. The number of time slots in this time space will be 4.

3. Determining Time and Context based Riskiness for Decision Making

As discussed before the trusting peer while assimilating the recommendations should also consider the following:

- The time spot at which the recommending peer interacted with the trusted peer. As mentioned in the previous section, Risk is dynamic and hence the trusting peer should give more weight to recommendations which are in the same time slot.
- The trusting peer should consider recommendations from peers who are either trustworthy or unknown recommenders and discard the recommendations from those peers who give un-trustworthy recommendations.

Hence in order for the trusting peer to decide with which trusted peer to interact with it should consider these scenarios when it assimilates the recommendations and determines the Riskiness value of each trusted peer. In order to get a better understanding of the proposed concept let us consider that a trusting peer 'A' wants to interact with a trusted peer in the context of transporting its goods from one place to another. Let us assume that the criteria of trusting peer 'A' in the interaction are C1, C2 and C3. The trusting peer 'A' has not interacted before in this context with any trusted peer and hence broadcasts its request of transporting its goods. Let us suppose that it gets replies from peers 'B' and 'C' who are willing to fulfill peer 'A' request. These peers are the set of possible trusted peers from which the trusting peer has to decide and choose one of them to interact with. Since the trusted peer has not interacted with any of these possible peers before, it does not know the Risk that could be associated in dealing with each peer. Hence in order to analyze the Risk involved in dealing with each trusted peer and ease its process of decision making it asks for recommendation from other peers. The peers who had interacted with the trusted peers in question reply back with their recommendations in the form of Risk set.

After getting the recommendations, the trusting peer should assimilate the recommendations according to the criteria, time and trustworthiness and determine the Riskiness value of the trusted peers accordingly. Based on the Riskiness value achieved for the trusted peers, the trusting peer can decide with which trusted peer to interact with.

As discussed earlier each recommending peer might have their own criteria in its interaction with the trusted peer and the Riskiness value that it recommends for the trusted peer is based on its assessment of un-commitment by the trusted peer in those criteria. Hence the trusting peer while assimilating the recommendations must consider only the criterion of interest in its interaction from the recommendations and determine the Riskiness value of the trusted peers in each criterion according to those recommendations. It can then determine the final Riskiness value of the trusted peers according to its criteria by weighting the Riskiness value of each criterion by the significance of the criterions.

The Riskiness value of a particular trusted peer ‘P’ in criterion ‘C’ (R_{PC}) can be determined after assimilating the recommendations by using the following formulae:

Riskiness value of the trusted peer ‘P’ in Criterion C (R_{PC}) =

$$(\alpha * ((\frac{1}{N} * \left| \gamma*(\sum_{i=1}^{N} \text{RRP}_i * \text{Commitment Level}_i) \right|)+ (\frac{1}{K} * \left| \delta *(\sum_{l=1}^{K} \text{RRP}_l * \text{Commitment Level}_l) \right|)))$$

$$+$$

$$(\beta * ((\frac{1}{J} * \gamma (\sum_{o=1}^{J} \text{Commitment Level}_o)) + (\frac{1}{M} *\delta (\sum_{q=1}^{M} \text{Commitment Level}_q))))$$

Equation-------1

where RRP_i is the Riskiness value of the trustworthy recommending peer i, whose recommendation is in the recent time slot of the trusting peer’s interaction,

RRP_l is the Riskiness value of the trustworthy recommending peer l, whose recommendation is in the far recent time slot,

Commitment level $_c$ is the level of commitment by the trusted peer in the particular criterion ‘c’ as recommended by the recommending peer in its recommendations,

N and K are the number of trustworthy recommendations classified according to the time slot of the recommendations,

J and M are the number of unknown recommendations classified according to the time slot of the recommendations,

γ and δ are the weights attached to the parts of the equation which give more weight to recommendations which are in the recent time slot as compared to the far recent ones . In general $\gamma > \delta$ and $\gamma + \delta = 1$,

α and β are the weights attached to the parts of the equation which will give more weight to the recommendation from the trustworthy recommending peers as compared to the unknown recommending peers. In general $\alpha > \beta$, and $\alpha+\beta=1$.

The first part of the above equation calculates the Riskiness value of the trusted peer ’P’ in a criterion ‘C’ by taking the recommendations of the trustworthy recommending peers and the second part calculates the Riskiness value of the same trusted peer in the same criterion ‘C’ by taking the recommendations of the unknown recommending peers. The recommendations from the untrustworthy recommending peers are left out and not considered. Further the Riskiness value determination of the trusted peer by taking the recommendations of the trustworthy and the unknown recommending peers too is done in two parts according to the time slot of the recommendations. The trusting peer should give more weight to the recommendations which are in the recent time slot of its interaction as compared to the far recent time slot recommendations. Those weights are represented by γ and δ respectively. In order to give more importance to the recommendations from the trustworthy recommending peers as compared to the recommendations from the unknown recommending peers, weights are attached to the two parts of the equation. These weights are represented by α and β respectively. It depends upon the trusting peer on how much weight does it want to give to each recommendation. By multiplying the Riskiness value of the recommending peer (RRP) with the commitment level that it is suggesting for a criterion we are getting the accurate recommendation according to its Riskiness.

As mentioned earlier any recommending peer whose Riskiness value while giving recommendations is with in the range of (-1, 1) is said to be a trustworthy recommending peer. So it is possible that the Riskiness value for the trusted peer in a criterion ‘C’ calculated from the trustworthy recommendations might come negative. We take the range of (-1, 1) to determine whether the recommendation is trustworthy or not and once it has been determined, it should not have any effect in determining the final Riskiness value of the trusted peer in a criterion by assimilating the recommendations. Hence we apply the *mod* operator to the first part of equation 1 which determines the Riskiness of the trusted peer in a criterion ‘C’ by taking the trustworthy recommendations.

In order to map the Riskiness value (R_{PC}) of the trusted peer ‘P’ in a criterion ‘C’ on the Riskiness scale (RS), it should be multiplied by 5. Hence Riskiness value of the trusted peer ‘P’ in a criterion ‘C’, mapped to the Riskiness scale (R_{PRSC}) is:

$$R_{PRSC} = \text{ROUND} (R_{PC} * 5)$$ **Equation--------2**

When the Riskiness value in each criterion of the trusting peer’s interaction has been determined on the Riskiness scale for the trusted peer by assimilating the recommendations, then the final Riskiness value of the trusted peer in the interaction can be determined by weighing the individual Riskiness value of each criterion according to its significance, depending on the trusting peer. The levels of significance for each criterion (Sc) are shown in table 1. The significance of each criterion in an interaction might depend on the degree to which it influences the successful outcome of the interaction according to the trusting peer.

Significance level of the Criterion (Sc)	Significance Rating and Semantics of the level
1	Minorly Significant
2	Moderately Significant
3	Largely Significant
4	Majorly Significant
5	Highly or Extremely Signifcant

Table 1 showing the significance level of each criterion

Hence the final Riskiness value (CR_P) of the trusted peer 'P' according to the criteria and significance of each criterion in the interaction by soliciting recommendations from other peers can be calculated as:

$$CR_p = \text{ROUND} \left(\frac{1}{\sum_{c=1}^{n} Sc} \left(\sum_{c=1}^{n} Sc * R_{PRSC} \right) \right)$$

Equation-----3

Where Sc is the significance of the criterion 'C'

R_{PRSC} represents the Riskiness value of the trusted peer 'P' in criterion 'C' on the Riskiness scale

n is the number of criterions in the interaction.

It should be noted that the Riskiness value of the trusted peer (CR_p) determined by assimilating the recommendations should be set to 0 if it is less than 0, as the Riskiness scale ranges from 0 to 5 with a value of -1 as Unknown Risk .

Finally when the trusting peer 'A' calculates the Riskiness values of the trusted peers 'B' and 'C' according to the criterions of its interaction by using the above concept, then it can easily decide with which trusted peer to interact with depending on their Riskiness values.

4. Conclusion

In this paper we discussed and proposed a solution to the scenario of the trusting peer having to decide with which peer to interact with among a set of trusted peers. If the trusting peer hasn't interacted with any of the trusted peers before then it does not know the level of Risk that could be present in its interaction. We proposed a solution to this problem by analyzing Risk by soliciting recommendations from other peers and then assimilating them according to the trusting peer's criteria to determine the Riskiness value of the trusted peers on the Riskiness scale.

5. References

[1] H. Chan, R. Lee, T.S. Dillon and E. Chang (2002), *E-Commerce and its Applications,* 1 edition, John Wiley and Sons, Ltd.

[2] R.M. Adler, 'Distributed Coordination Models for Client/Sever Computing. *Computer 28,* 4 pp. 14-22, 1995.

[3] B. Leuf (2002), '*Peer to Peer, Collabration & Sharing on the Interent'*, Pearson Education Pty Ltd.

[4] A. Oram, 'Peer-to-Peer: Harnessing the Power of Disruptive Technologies' Retrieved 16 February, 2004, Available: *http://www.oreilly.com/catalog/peertopeer/chapter/ch01.html.*

[5] S. Greenland, 'Bounding analysis as an inadequately specified methodology', *Risk Analysis,* vol. 24, no. 5, pp. 1085-1092, 2004.

[6] J.G. March and Z. Shapira, 'Managerial perspective on risk and risk taking', *Management Science*, vol. 33, no. 11, pp. 1404-1418, 1987.

[7] M. E. Orlowska, 'The Next Generation Messaging Technology – Makes Web Services Effectives', *Proceedings of the Sixth Asia Pacific Web Conference*, pp. 13-19, Springer-Verlag, Berlin Heidelberg 2004.

[8] C. Qu, and W. Nejdl, 'Interacting the Edutella/JXTA Peer-to-Peer Network with Web Services', *Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp* 67, 2004.

[9] C. Schmidt, and M. Parashar, 'A Peer-to-Peer Approach to Web Service Discovery', *World Wide Web Journal*, Vol. 7, Issue 2, pp. 211-229, 2004.

[10] C. Schuler, R. Weber, H. Schuldt, and H. Schek, 'Scalable Peer–to–Peer Process Management — The OSIRIS Approach', *Proceedings of the IEEE International Conference on Web Services,* San Diego, USA, pp.26, 2004.

[11] M. Ripeanu, 'Peer-to-Peer Architecture Case Study: Gnutella Network', *Proceedings of the First International Conference on Peer-to-Peer Computing* , pp 99-100, 2001.

[12] M.P. Papazoglou, B.J. Kramer, and J. Yang, 'Leveraging Web-Services and Peer-to-Peer Networks', Springer-Verlag Berlin Heidelberg 2003.

[13] O.K.Hussain, E. Chang, F.K. Hussain, T.S. Dillon and B. Soh, 'A Methodology for Determining Riskiness in peer-to-Peer Communication', *Proceedings of the 3rd International IEEE Conference on Industrial Informatics*, pp 421-432, 10-12 August 2005.

[14] O.K Hussain, E.Chang, F.K. Hussain, T.S. Dillon and B. Soh, "Modeling the Risk Relationships and Defining the Risk Set (Accepted for publication)," CollECTeR Latam 2005, to be published.

[15] O.K. Hussain, E. Chang, B. Soh, F.K. Hussain, and T.S. Dillon 'Factors of Risk Variance in Decentralized Communications', *European Institute of Computer Antivirus Research*, Malta, 30 April-3 May 2005,pp 162-170.

[16] O.K. Hussain, E. Chang, F.K.Hussain, T.S. Dillon and B. Soh. "Risk in Trusted Decentralized Communications", *Proceedings of the International Workshop on Privacy Data Management in Conjunction with 21st International Conference on Data Engineering (ICDE PDM 2005) pp 63-67,* Tokyo, Japan, 9 April 2005.

[17] J. Carter and A.A. Ghorbani, 'Towards a formalization of Trust' *Web Intelligence and Agent Systems,* Vol. 2, No. 3, pp. 167-183, March 2004.

[18] O.K Hussain, E. Chang, F.K. Hussain, T.S. Dillon and B. Soh, "Context Based Riskiness Assessment" (Accepted for publication), IEEE TENCON 2005, to be published, Melbourne, Australia, 2005.