Reprinted from:

2005 3rd IEEE International Conference on Industrial Informatics (INDIN) Perth, Australia 10-12 August 2005

IEEE Catalog Number ISBN 05EX1057
ISBN 0-7803-9094-6

A Methodology for Determining Riskiness in Peer-to-Peer Communications

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, W.A., Australia
e-mail :{ Omar.Hussain, Elizabeth.Chang, Farookh.Hussain}@cbs.curtin.edu.au
[2] Faculty of Information Technology, University of Technology, Sydney, NSW, Australia
e-mail: tharam@it.uts.edu.au
[3] Dept of Computer Science and Computer Engineering, La Trobe University, VIC, Australia
e-mail: ben@cs.latrobe.edu.au

Abstract---**Every activity has some Risk involved in it. Analyzing the Risk involved in a transaction is important to decide whether to proceed with the transaction or not. Similarly in Peer-to-Peer communication analyzing the Risk involved in undertaking a transaction with another peer too is important. It would be much easier for the trusting peer to make a decision of proceeding a transaction with the trusted peer if he knows the Risk that the trusted peer is worthy of. In this paper develop and propose such a methodology which allows the trusting peer to rate the trusted peer in terms of Risk that he deserves after the transaction is over.**

Index Terms ---- **Riskiness, Interaction, Criterion, Trusting peer and Trusted peer.**

I. INTRODUCTION

Decentralized transactions are increasingly becoming popular. These transactions resemble the early forms of the internet and in many ways are regarded as its next generation. The result will be that the e-commerce transactions approach will shift from the current client-server environment to peer-to-peer communications [1]. However, these peer-to-peer communications or decentralized transactions suffer from some disadvantages, which includes risk associated with each transaction. 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 [2]. Thus it commands a central role in any discussion of e-commerce that is related to a transaction. There has been an extensive discussion in the literature on Risk that is present in a transaction [3]. Some define Risk by the magnitude of its outcome rather than its likelihood [4], where as some define the presence of Risk in the transaction where the possible damage is more than the advantage sought [5, 6]. Some researchers see Risk as the potential negative consequences and hence the probability of the failure [7, 12] where as some see it as the probability of the loss in the resources invested [8]. At the start of a transaction the consumer will be uncertain on how the transaction might proceed. [9] takes into account this uncertainty and defines Risk as the consumer's perception of the uncertainty and adverse consequence of engaging in an activity. [10, 11] defines Risk as having 2 dimensions. One relates to uncertainty and the other relates to the consequence of the importance of the notion of loss.

II. THE CONTRAST BETWEEN RISK AND TRUST

It is clear that Risk & Trust are dependent on each other, but it is still unclear whether Risk is an antecedent to Trust or an outcome of Trust. For example it can be said that in an interaction Risk creates an opportunity for Trust which leads to Risk taking. In this case Risk is an antecedent to Trust. But it can also be said that when the interaction is done based on the level of Trust, then there is a low amount of Risk in it. In this case Risk is an outcome of Trust. Risk can provide a moderating relationship between Trust and the behavior of the peer in an interaction. For example the effect of Trust on the behavior is different when the level of Risk is low and different when the Risk is high. Similarly Risk can have a mediating relationship on Trust. For example the existence of Trust reduces the perception of Risk which in turn improves the behavior in the interaction and willingness to engage in the interaction. Finally

0-7803-9094-6/05/$20.00 ©2005 IEEE

Trust and Risk are two different components that complement each other. The higher the trust the lower the Risk and vice versa

After an interaction is complete if would be better if the trusting peer rates the Risk involved in dealing with the trusted peer, so that it gives an indication to other peers of the Risk involved in dealing with this peer. In this paper we try and propose such a methodology, by assigning the peers with a *Riskiness* value. This will enable the trusting peer or any other peer to know before hand the amount of Risk that would be present in dealing with this peer. We define what the term *Riskiness* means and then define seven different Riskiness levels. Further we define the semantics associated with those levels and propose a methodology by using the proposed metrics, which the trusting peer uses to assign a Risk value to the trusted peer after the interaction.

III. DEFINING THE TERM RISKINESS

We define the term Riskiness as *the numerical value that is assigned by the trusting peer to the trusted peer after the transaction, which shows the amount of Risk that the trusted peer is worthy of on the Riskiness scale.*

It also quantifies the amount of Risk present in the transaction. The numerical value corresponds to a level on the Riskiness scale, which gives an indication to other peers about the nature of the trusted peer and up to what level of Risk is present in dealing with that peer.

IV. RISKINESS LEVELS AND THEIR SEMANTICS

In this section we present the different Riskiness levels, their values and their semantics which explain the meaning of these levels.

Levels of Riskiness and their Values.

In table 1 we define 7 different levels of Riskiness and their corresponding semantics in the domain (-1, 5). The domain of Riskiness is defined as the set of values from which the trusted peer is assigned a value by the other peers that shows the Risk in dealing with that trusted peer.

V. SEMANTICS OF THE RISKINESS LEVELS AND THEIR POSTULATES

In this section we define the different Riskiness levels and propose the semantics that are associated

Table 1 showing the seven levels of Risk and the corresponding star visual representation

Riskness Levels	Semantics (Linguistic Definitions)	Riskness Value (User defined)	Visual Representation (Star Rating System)
Level -1	Unknown Risk	$x=-1$	Not displayed
Level 0	Very Risky	$x=0$	Not displayed
Level 1	Risky	$0<x\leq 1$	From ½ to ★
Level 2	Partially Risky	$1<x\leq 2$	From ★½ to ★★
Level 3	Largely UnRisky	$2<x\leq 3$	From ★★½ to ★★★
Level 4	UnRisky	$3<x\leq 4$	From ★★★½ to ★★★★
Level 5	Very UnRisky	$4<x\leq 5$	From ★★★★½ to ★★★★★

with each of these levels and the postulates for those levels. Postulates define the possible scenario by which the trusted peer might get this level.

A. Level -1.

Level -1 is the first level of the Riskiness scale. It is termed as *Unknown Risk.*

Semantics: This value is assigned to the trusted peer [14] by any peer giving recommendation if they cannot make an informed decision about the Riskiness value of the trusted peer. So we propose that instead of assigning any random Riskiness value with in the range of (0, 5), a Riskiness value of -1 be assigned to the trusted peer.

A Riskiness value of -1 implies that the recommending peer assigning the value does not have any idea about the Riskiness of the trusted peer and is ignorant about it. An important point to note is that all new peers in a network begin with this value, and hence a Riskiness value of -1 is assigned to the trusted peer, when there are no precedents that can help the trusting peer to determine the Riskiness level of the trusted peer.

Postulates: The following are the conditions under which the trusted peer can be assigned a Riskiness value of '-1'.

- The trusted peer is new to Peer-to-Peer network.
- The trusting peer does not have any previous interaction with the trusted peer and hence is not in a position to determine the Riskiness of the trusted peer.

- All the other peers which give recommendation to the trusting peer did not carry out interaction with the trusted peer before and hence cannot define the Riskiness value.

B. Level 0

Level 0 is the second level in the Riskiness scale and it is termed as *Very Risky*.

Semantics: This value is assigned to the trusted peer by the trusting peer after the interaction or any other peer giving the recommendation when they think that at a given point of time and at a given context the trusted peer is completely unreliable to perform a given action, or the trusted peer acts completely in a fraudulent way. In other terms he does not behaves in the interaction according to the expected behavior or mutually agreed behavior at all and acts fraudulently in the interaction, hence increasing the Risk by a greater extent in the interaction. A Riskiness value of 0 expresses the largest level of high Risk.

It is anticipated that a peer who is assigned a Riskiness value of 0, in future interactions will behave in exactly the same way as expected by the trusting peer or speaking in other terms in the same way he behaved in this interaction.

A peer which has been assigned a Riskiness value of 0 is defined as *Very Risky* peer

Postulates: The following are the conditions in which the trusted peer can be assigned a Riskiness value of 0

- The trusted peer has behaved very fraudulently with the trusting peer or with any other peer who has given the recommendation about the trusted peer.
- The trusting peer had communicated all the factors or bases against which its Riskiness is going to be analyzed and he did not fulfill any one of those.
- A majority of the other recommending peers have given the Riskiness value of 0 to the trusted peer.

C. Level 1

Level 1 is the third level in the Riskiness scale and it is termed as *Risky*.

Semantics: This value is assigned to the trusted peer by the trusting peer after the interaction or any other peer giving the recommendation when they think that at a given point of time and at a given context the trusted peer is unreliable to perform a given action. In other terms he deviates from the expected behavior or mutually agreed behavior most of the times, hence increasing the Risk accordingly too. A Riskiness value of 1 expresses the lesser level of high Risk.

It is anticipated that a peer who is assigned a Riskiness value of 1, in future interactions would behave in a nearly the same way as it has done in this interaction.

A peer which has been assigned a Riskiness value of 1 is defined as a *Risky peer.*

Postulates: The following are the conditions in which the trusted peer can be assigned a Riskiness value of 1

- The recommendations of the recommending peer assigned a Riskiness value of 1 to the trusting peer.
- The trusting peer deviated from the expected behavior most of the times.
- The trusting peer had communicated all the factors or bases against which its Riskiness is going to be analyzed.

D. Level 2

Level 2 is the fourth level of the Riskiness scale and it is termed as *Partially Risky.*

Semantics: A Riskiness value of 2 signifies a level of risk, which leans more to the negative side (Level 0&1). A Riskiness value of 2 would indicate that the behavior of the trusted peer in the interaction with the trusting peer was such that it can neither be regarded as good nor bad. In other words it can neither be classified as Risky nor Un-Risky. A Riskiness value of 2 expresses a lesser level of neutral risk.

It is anticipated that the peer who has been assigned a Riskiness value of 2, will behave in a way which is capable for neutral Risk or worse than that (levels 0&1) in future interactions.

The peer which has been assigned a Riskiness value of 2 is defined as *Partially Risky Peer.*

Postulates: The following are the conditions in which the trusted peer can be assigned a Riskiness value of 2

- The trusting peer had been communicated MOST or ALL the bases on which the Riskiness of the trusted peer will be evaluated.
- The majority of the other peers which gave recommendation to the trusting peer assigned a Riskiness value of 2 to the trusted peer.
- The trusted peer neither acted in a fraudulent way (levels 0&1) nor in an un-risky way (levels 4&5).

E. Level 3

Level 3 is the fifth level of the Riskiness scale. It is termed as *Largely Un-Risky.*

Semantics: This value is assigned to the trusted peer by the trusting peer after the interaction. Alternately any peer may make this recommendation at a given context and at a particular time suggesting that the trusted peer can be relied upon to complete a task up to a certain extent. Broadly speaking this type of Risk can be termed as neutral Risk, but this neutral risk leans more to the positive side (Levels 4 & 5). Hence a Riskiness value of 3 expresses the larger level of neutral Risk.

A Riskiness value of 3 shows that the behavior of the trusted peer with the trusting peer can neither be regarded as good (Level 4&5) nor regarded as bad or unacceptable (Level 0&1). In other words the trusting peer acted in neither an un-risky nor in a risky way. It is anticipated that the peer who has been assigned a Riskiness value of 3, will behave in a way which is capable for neutral Risk or better than that (levels 0&1) in future interactions.

A peer which has been assigned a Riskiness value of 3 is defined as *Partially Risky Peer.*

Postulates: The following are the conditions in which the trusted peer can be assigned a Riskiness value of 3

- The majority of the other peers making recommendation to the trusting peer assigned a Riskiness value of 3 to the trusted peer.
- The trusted peer neither acted in a fraudulent way (levels 0&1) nor in an un-risky way (levels 4&5).
- The trusting peer might not have been communicated MOST or ALL the bases against which the Riskiness of the trusted peer will be evaluated.

F. Level 4

Level 4 is the sixth level of the Riskiness scale. It is termed as *Un-risky.*

Semantics: This value is assigned to the trusted peer by the trusting peer at the conclusion of the interaction. It can also be assigned by other peers at any time and in any setting once it becomes clear that the trusted peer can be relied on to perform a give action. In other words he completes MOST but not ALL of the actions according to expected behavior or mutually agreed behavior, and hence there is some amount of Risk involved in the interaction. A Riskiness value of 4 indicates that the trusted peer assigned with this value can be relied on to a large extent in a given context to complete the interaction, but not relied completely as compared to level 5.

It is anticipated that the peer who has been assigned a Riskiness value of 4, will behave in nearly the same way as expected by the trusting peer in the future interactions or improve its behavior which could assign it a Riskiness value of the next level, i.e. level 5.

A peer which has been assigned a Riskiness value of 4 is defined as *Un-Risky peer.*

Postulates: The following are the conditions in which the trusted peer can be assigned a value of 4 on the Riskiness scale.

- The trusted peer fulfills most but not all of the tasks according to the expected behavior
- The recommendations given by the others peers to the trusting peer have assigned a Riskiness value of 4 to the trusted peer.

G. Level 5

Level 5 is the seventh and last level of the Riskiness scale. It is termed as *Very Un-Risky.*

Semantics: This value is assigned to the trusted peer by the trusting peer after the interaction or by other peers giving the recommendation when they think that at a given point of time and context, the trusted peer can fully be relied upon to perform a given action. This is to say that he completes his actions EXACTLY according to expected behavior or mutually agreed behavior and the interaction is totally safe. If there is any Risk in this interaction then it will be minimal. A Riskiness value of 5 indicates that the trusted peer assigned with this value can be relied upon completely in a given context to complete the interaction.

It is anticipated that the peer who has been assigned a Riskiness value of 5, will behave in exactly the same way as expected by the trusting peer in future interactions i.e. in the same way as it acted in this interaction. This level defines the absence of Risk in the interaction or if any present then the lowest possible amount of Risk that can be involved in the interaction. This is the highest possible level which represents an un-risky interaction and it is the larger level of low Risk.

A peer which is assigned a Riskiness value of 5 is defined as *Very Un-Risky Peer.*

Postulates: The following are the conditions in which the trusted peer can be assigned a Riskiness value of '5'

- The trusted peer fulfills all that is expected from the trusting peer for this interaction. Or

in other terms the trusted peer might act exactly according to the expected or agreed behavior

- All the other peers from whom the trusting peer receives the recommendation have given a Riskiness value of 5 to the trusted peer.

VI. ASSIGNING A RISKINESS VALUE TO A TRUSTED PEER

The Riskiness value that the trusted peer gets from other peers is dependent on a number of factors, as Risk too varies according to different factors [13]. These factors for determining the Riskiness of the trusted peer are not the same for all the Peer-to-Peer communications. They vary according to each interaction. Even in a single interaction the basis for determining the Riskiness of the peer depends on a number of criterions and how the trusted peer reacts in each of the criterion. The sum of the commitment of each criterion with relative to the best possible commitment is the final value which is assigned to the trusted peer as the Riskiness Value.

For example let us consider the interaction between Alice and Bob regarding the context of MP3 player. Alice wants to buy a MP3 player of a specific model and of a specific colour and queries all the other peers regarding the availability of the player. Bob replies back confirming the availability of that specific player and agree to sell it to Alice. So the criteria on which Alice is going to determine the Riskiness of Bob is

- Whether Bob sells the MP3 player of the specific model which Alice wants.
- Whether the MP3 player is of the same colour that Alice wants.

Hence the criteria for determining Bob's riskiness as a provider in this interaction depends on these factors specified by Alice, and up to what level does Bob fulfill these factors.

Our method of assigning Riskiness to a peer is through the notion of *expectations* i.e. the expected behaviour or what was agreed, the Mutually Agreed Behaviour and *commitment* i.e. to what extent the trusted peer commits to the expected behaviour. In other terms it can be said as expected behaviour Vs actual behaviour. The greater the difference between these two behaviours the higher the level of Risk present in the interaction and vice versa.

In other words arriving at a level of risk rating can be seen as an interaction between both the trusted and trusting peer. If the trusted peer behaves in a mutually agreed fashion they warrant a corresponding riskiness value. In order to measure the degree of commitment and assign a corresponding Riskiness value to the trusted peer after the interaction, the trusting peer will make use of the CCAS metrics. If the trusting peers expectations are met then a corresponding favourable score to the trusted peer will be assigned by the metrics.

VII. METRICS FOR ASSIGNING A RISKINESS VALUE TO A TRUSTED PEER

In this section we will define the metrics for finding out the Riskiness of a peer. As mentioned in the previous section the method of assigning Riskiness to a peer is through the notion of *expectations* and *commitment* with regard to those expectations.

By *Expectations* we mean the expected behavior. This is the way in which the trusting peer thinks that the interaction will proceed [16]. *Expectations* also refer to mutually agreed behavior that is the promised commitment from the trusted entity.

By *Commitment* we mean the degree to which the actual behavior correlates with the expected behavior. This will tell us how the trusted peer actually behaved in the interaction and how much did he commit to the expected behavior. If the trusting peer measures the level of commitment by CCAS metrics and maps this degree of commitment to the Riskiness scale then it will get the Riskiness value of the trusted peer.

H. Metric 1: Commitment in an Interaction (Com $_{Interaction}$)

We represent the commitment in an interaction by Com $_{Interaction.}$ As mentioned before each interaction consists of a number of criteria. Hence the total commitment in the interaction Com $_{Interaction}$ can be found by:

- Determining the commitment in the behavior of each criterion of an interaction.
- Adding up all the commitments of the criteria to get the total commitment in the Interaction (Com $_{Interaction}$).

To explain this with an example let us consider an interaction between Bob and Alice in the context of MP3 player as explained before. Alice will assign a Riskiness value to Bob based on:

- Whether Bob sells the MP3 player of the specific model which Alice wants.
- Whether the MP3 player is of the same colour which Alice wants.

These are the criteria which are responsible for assigning a Riskiness value to Bob based on how he reacts in them. The commitment in the interaction will be ascertained by finding out the commitment in each criterion. Hence we represent the commitment in each criterion as $Com_{Criterion}$.

Hence the commitment of the interaction in this case can be found out by

- Determining the commitment in the behavior of Bob in selling the MP3 player of the specific model to Alice which she wants (Com_{Model})
- Determining the commitment in the behavior of Bob in selling the MP3 player of the same colour to Alice which she wants (Com_{Colour})

Therefore commitment 1 = *model,* commitment 2 = *colour.* These two individual values show the commitment in these criterions. The total commitment in the interaction can be found out by adding the commitment in these criterions, i.e. $Com_{Model} + Com_{Colour}$.

Hence the total commitment in an interaction can be found out by adding the individual commitment in each criterion.

$$Com_{Interaction} = \sum_{I=1}^{N} (Com_{Criterion\ I})$$

where I is the number of criterions in an interaction.

I. Metric 2: Commitment in a Criterion ($Com_{Criterion}$)

The $Com_{Criterion}$ is measured as the commitment in the actual behavior of the trusted peer in regard to the expected behavior of the trusting peer in a criterion. In the end the commitment in a criterion ($Com_{Criterion}$) should be a numeric value which is achieved by mapping to its level, and which in turn shows whether the trusted peer performed the actions as expected by the trusting peer or not.

Considering the above example of the interaction between Bob and Alice, the commitment in the criterion (Com_{Model} and Com_{Colour}) can be arrived at by:

- Determining whether Alice got the MP3 player of the same model she actually wanted.
- Determining whether the colour of the MP3 player which Alice got is the one she actually wanted.

In order to express or compare the commitment of the actual behavior from the expected behavior we define two levels of $Com_{Criterion}$. Those levels are explained in the next section.

As explained earlier while considering the commitment of a criterion and assigning a Riskiness value to the trusted peer, it is also important to consider some other factors too. We will explain those factors in the next subsection and define metrics to measure them.

J. Metric 3: Accuracy of the Criterion Communication ($Accu_{Criterion}$)

Riskiness can be correctly analyzed when the trusted peer knows all the factors and bases against which it will be analyzed. So it is important that the trusting peer communicates each of those factors clearly to the trusted peer beforehand in order to assign it a deserving Riskiness value.

Hence the Accuracy of the Criterion Communication metric ($Accu_{Criterion}$) can be defined as the metric which is used to express whether the factors or the bases against which the interaction is going to be judged or analyzed has been communicated to the trusted peer in clear terms or not.

To explain this with an example lets us consider the interaction between Alice and Bob and further assume that Bob knows the factors or the bases by which Alice is going to judge and assign him a Riskiness value. Suppose while assigning the Riskiness value to Bob, Alice considers the delivery mode which Bob used for sending the MP3 player and it is different to what Alice wanted. Then Bob might not get the actual Riskiness value that he should get or that he deserves because of the additional factor that was not communicated to him.

Hence each of the criteria or the factors by which the Riskiness of a peer is going to be judged should be clearly communicated before the interaction begins in clear terms. The metric which describes whether the factor has been communicated clearly or not is $Accu_{Criterion}$. We will define the different levels that show whether the factors that are responsible for the judgment of a criterion were communicated clearly to the trusted peer or not in the next section. This will be taken into consideration to find out the level of commitment of an individual criterion.

K. Metric 4: Significance of the Criterion ($Sig_{Criterion}$)

Another important factor to consider while finding out the commitment in an interaction is the Significance of the criterion ($Sig_{criterion}$). We define the metric $Sig_{criterion}$ which expresses the significance of that particular criterion and hence gives the trusted peer an idea of criterions which should be considered important for the interaction.

All the criteria of an interaction will not be of equal importance or significance. Some criteria might play an important role in determining the Riskiness of the peer and some might not be as crucial as others. The significance of each criterion in an interaction might depend on the degree to which it influences the successful outcome of the interaction. For example according to the trusting peer, some criteria might be there which will have an important effect in the completion of an interaction and some criterions will have a minimal result in the outcome of the interaction.

For example if we take the above interaction between Alice and Bob regarding the MP3 player. Alice will analyze Bob of the Riskiness value that he deserves on these factors:

- Whether Bob will send the MP3 player of the specific model which Alice wants.
- Whether the MP3 player is of the same colour which Alice wants.
- Bob will send the MP3 player to Alice by courier at the end of the interaction.

Let us assume that the first two factors are very important to Alice in the interaction with Bob and she is not bothered of how Bob sends the MP3 player to her. Hence she might focus on the first two factors in determining the commitment of the actual behavior in regard to the expected behavior and finding the Riskiness value.

For example let us assume that this same interaction is taking place between John and Mary, who are the trusting and trusted peer respectively. But according to John all the above factors are important in deciding about the Riskiness value of Mary, and he might take all the factors into consideration while deciding about the Riskiness value.

Thus the importance or the significance of each criterion should be clearly mentioned to the trusted peer in order to rate its Riskiness value correctly. One more dis-advantage of not mentioning the importance of the factors is that the trusted peer will fulfill the factors which are un-important in determining the Riskiness value and leave the other factors which form the core for accessing the Riskiness value.

In the next section we will define the levels which will shows how important that criterion is for the interaction.

VIII. LEVELS FOR THE METRICS DEFINED

In this section we define the proposed levels for the metrics defined in the previous section, namely $Com_{Criterion}$, $Accu_{criterion}$ and $Sig_{criterion}$. Using these values of the respective levels we will derive the value of $Com_{Interaction}$ in the next section.

L. Levels of Com Criterion

In order to assign a correct Riskiness value to the trusted peer, the trusting peer will need to find out whether a particular interaction has been fulfilled in accordance with the expected behavior. For that we define two levels for $Com_{criterion}$. Each of those two levels corresponds to a different level or degree which shows the level of fulfillment of each criterion. A numerical value is assigned to each level, and the value which corresponds to the level of how the criterion was fulfilled by the trusted peer is taken into consideration while determining its Riskiness. The levels are explained in table 2.

M. Levels for Accu Criterion

We believe that a criterion should be taken into consideration by the trusting peer while determining the Riskiness of the trusted peer only if the bases or the factors that the trusting peer will use to judge the behavior of the trusted peer in that criterion, have been communicated to the trusted peer in clear terms. So in order to determine the accuracy of the factors which have been communicated to the trusted peer by the trusting peer, we define two levels for the metric $Accu_{criterion}$. The numerical value which corresponds to the level of accuracy by which the metrics were defined will be taken into consideration, while finding out the Riskiness of the peer. The levels are explained in table 3.

N. Levels of Sig Criterion

The metric Significance of the criterion ($Sig_{Criterion}$) depicts how important the trusting peer thinks the criterion is in the completion of the interaction. The Significance of each criterion will be taken into account in determining the Riskiness of a trusted peer. The trusting peer will assign a significance level that he thinks is appropriate to each criterion. The numerical value which corresponds to that level of significance will be taken into account while finding the Riskiness of the trusted peer. So in order to assign a significance value to the criterion we define three levels for the metric $Sig_{Criterion}$. Those levels are explained in table 4.

IX. DETERMINING THE COMMITMENT IN THE WHOLE INTERACTION ($COM_{INTERACTION}$)

Table 2 showing the levels for the metric Com $_{Criterion}$

Com $_{Criterion}$ Value	Semantics of the Value
0	The trusted peer's commitment for this criterion was not as it was expected from him according to the expected behavior or as it was promised first according to the mutually agreed behavior.
1	The criterion proceeded exactly according to the expected behavior, i.e. there is no deviation between the actual behavior and the expected behavior and the commitment of the trusted peer was as expected or promised.

Once a value from each metric defined above is assigned to each criterion, then the total commitment in the whole interaction can be determined. As explained before the total commitment in the interaction Com $_{Interaction}$ will take into consideration

- The criteria against which the commitment is going to be measured
- The amount of commitment of all those criterions Com $_{Criterions}$
- The accuracy by which those criterions were communicated to the Trusted peer Accu $_{Criterion}$
- The Significance of each criterion that it will have on the interaction and while determining the Riskiness of the peer Sig $_{Criterion}$.

Table 3 showing the levels for metric Accu $_{Criterion}$

Accu $_{Criterion}$ Value	Semantics of the Value
0	The factors against which the criterion is going to be judged in order to determine whether it has been completed according to the promised commitment or the expected behavior has NOT been communicated to the trusted peer in clear terms.
1	The factors against which the criterion is going to be judged in order to determine whether it has been completed according to the promised commitment or the expected behavior HAS BEEN communicated to the trusted peer in clear terms

Table 4 showing the levels for metric Sig $_{Criterion}$

Sig $_{Criterion}$ Value	Semantics of the Value
0	The Criterion is not so important in determining the Riskiness of the peer
1	The criterion of this value is important and will have some significance in determining the Riskiness of the trusted peer. But there are other criterions apart from this which will have a major effect in determining the Riskiness of the peer.
2	A criterion of this value has the highest level of significance in determining the Riskiness of the peer and will play an important effect in determining the Riskiness of the peer.

Hence the commitment of the whole interaction can be expressed by:

$$\text{Com}_{Interaction} = \sum_{i=1}^{N} f(\text{Com}_{Criterion\,i}, \text{Accu}_{Criterion\,i}, \text{Sig}_{Criterion\,i})$$

where i represent a particular criteria and N represents the number of criterions in the interaction.

The above equation indicates that the commitment in an interaction Com $_{Interaction}$ is:

- The sum of the commitment of each criterion in an interaction.
- And the commitment in each interaction is expressed as a function of the levels of accuracy and significance of each criterion.

So if there are three criterions in an interaction the commitment of the interaction (Com $_{Interaction}$) which shows the amount of commitment in the actual behavior can be calculated as:

$$Com_{Interaction} =$$

$$(Com_{Criterion\,1} * Accu_{Criterion\,1} * Sig_{Criterion\,1}) +$$

$$(Com_{Criterion\,2} * Accu_{Criterion\,2} * Sig_{Criterion\,2}) + \text{-------} \quad 1$$

$$(Com_{Criterion\,3} * Accu_{Criterion\,3} * Sig_{Criterion\,3})$$

X. MAPPING THE COM $_{INTERACTION}$ VALUE TO THE RISKINESS SCALE

To find out the Riskiness of the trusted peer, the trusting peer needs to find out the degree of fulfillment between the committed behavior i.e. the

actual behavior in an interaction relative to the best possible commitment that could have been shown by the trusted peer i.e. expected behavior or the mutually agreed behavior.

The value that the trusting peer gets for $Com_{Interaction}$ is dependent on the behavior of the trusted peer. The larger the deviation in the behavior of the trusted peer from the expected behavior the lower the value of $Com_{Interaction}$ and vice versa. So in other terms $Com_{Interaction}$ depicts how the trusted peer behaved in the interaction. Once the trusting peer gets the value of $Com_{Interaction}$ it needs to map it to the Riskiness scale in order to find out the Riskiness of the trusted peer.

In order to properly quantify the $Com_{Interaction}$ to the Riskiness scale, the trusting peer needs to first find out how much the trusted peer's committed behavior is far from the best possible behavior expected. If it expresses the behavior of the trusted peer relative to the best possible behavior, then it will get a measure that quantifies the behavior of the trusted peer relative to the best possible behavior.

The best possible behavior in an interaction is possible when the trusted peer completes the interaction according to the expected behavior or according to the promised commitment of the mutually agreed behavior. Hence we define the best possible behavior as the promised commitment which the trusted entity makes before the interaction. We represent it as $ProCom_{Interaction}$ which shows a numerical value that quantifies the maximum possible commitment that could have happened between the actual behavior and the expected behavior.

We define $Risk_{Interaction}$ as the metric which expresses the numerical value of $Com_{Interaction}$ relative to $ProCom_{Interaction}$, and which gives the Risk involved in the interaction.

Hence $Risk_{Interaction}$ is expressed as

$$Risk_{Interaction} = \frac{Com_{Interaction}}{ProCom_{Interaction}} \quad \text{---------- 2}$$

In other terms $Risk_{Interaction}$ shows the amount of Risk that was there in the interaction to the trusting peer in dealing with the trusted peer. It shows the extent to which the trusted peer committed in the actual behavior from the expected behavior.

In order to find the Riskiness value of the trusted peer, the trusting peer needs to map the Risk involved in the interaction to the Riskiness scale, which is on a scale of (-1, 5). A trusting peer cannot assign the value of -1 to the trusted peer after it has completed the interaction, as -1 denotes that the trusted peer is new or unknown. This value is assigned to the trusted peer by any other peer giving recommendations when that peer does not know the Riskiness of the trusted peer, and after an interaction a value within the range of (0, 5) should be assigned to the trusted peer by the trusting peer. Hence the Riskiness of the trusted peer has to be mapped in the range of (0, 5) after the transaction. So in order to express the Riskiness value of the trusted peer on the scale (0, 5) Risk in the interaction, $Risk_{Interaction}$ should be multiplied by 5. The value obtained can be a real number. In order to express it as a whole number it has to be rounded off. Hence Riskiness is expressed as:

$$\text{Riskiness of the trusted peer} = ROUND\ (Risk_{Interaction} * 5)$$

This can also be written as:

$$\text{Riskiness Value} = ROUND\ \frac{Com_{Interaction}}{ProCom_{Interaction}} * 5 \quad \text{----- 3}$$

Or alternately speaking

$$\text{Riskiness Value} = ROUND \sum_{I=1}^{N} \frac{(Com_{Criterion\ I} * Accu_{Criterion\ I} * Sig_{Criterion\ I})}{(ProCom_{Criterion\ I} * Accu_{Criterion\ I} * Sig_{Criterion\ I})} * 5$$

where I represents the number of criterions in an interaction.

The proposed concept will become clear when we explain the method of finding Riskiness of the trusted peer in the next section by using an example.

XI. EXAMPLE FOR FINDING THE RISKINESS VALUE OF A PEER BY USING THESE METRICS

In this section we will explain the process of finding the Riskiness of a peer on the Riskiness scale by using the above metrics. To proceed further we will assume the following interaction in which Alice wants to buy a MP3 player. Thus Alice is the trusting peer in this interaction in the context of MP3 player. Bob replies to Alice saying that he is willing to sell his MP3 player and to proceed with the above interaction with Alice.

Alice and Bob discuss the interaction and arrive at the expected behavior or the mutually agreed

behavior. In other words, they agree on the promised commitment from the trusted peer.

Alice wants the following in the outcome of the interaction.

1. The MP3 player should be of brand *Sony*
2. It should be of red color
3. Its memory should be of at least 128 MB.
4. It's model should not be before then 2002
5. It should also be packed in its box while sending
6. Good Cosmetic Condition

This can also be referred to as the criteria in the above interaction.

Lets us suppose that this was the behavior from Bob in this interaction. This can be termed as actual behavior.

1. Sold an MP3 player of Sony brand to Alice
2. The MP3 player was of blue colour
3. Its memory was of 192 MB.
4. Model was of 2003
5. Did not send the MP3 player in its box to Alice.
6. The MP3 player had 3 scratches on it.

In order to determine the Riskiness of Bob, Alice will first determine how much did Bob commit in the actual behavior with respect to the expected behavior in each criterion. So the value of $Com_{Criterion}$ can be roughly calculated according to its metric as follows:

- For the first criterion Bob sent the MP3 player of Sony to Alice, and acted exactly according to the expected behavior. So the value of Com_{Brand} according to its level is 1.
- For the second criterion Alice wanted the MP3 player to be of red colour and Bob sold her an MP3 player of blue colour. So he deviated according to the expected behavior in the actual behavior. Hence the value of Com_{Colour} should be 0.
- For the third criterion Alice wanted the memory of the MP3 player to be at least 128 MB but got the MP3 player with a memory of 192 MB. So Bob acted according to the expected behavior. Hence the value of Com_{Memory} is 1.
- For the fourth interaction Alice wanted the model of the MP3 player not to be before than 2002, but Bob sold her a MP3 player of 2003 model. Hence the value of Com_{Model} in this case is 1.
- For the fourth interaction Alice wanted the MP3 player to be sent in its box to her, but Bob did not act accordingly. Hence the value of Com_{Box} is this criterion will be 0.
- For the fifth interaction Bob did deviate in providing the MP3 in good cosmetic condition. Hence the value of the $Com_{Condition}$ is 0.

Now after finding out the commitment in each criterion, the accuracy with which each criterion was communicated to Bob from Alice should be measured. So the value of $Accu_{Criterion}$ for each criterion is as follows:

- Criterion 1 was communicated clearly. Hence the value of $Accu_{Brand}$ is 1
- Criterion 2 was communicated clearly. Hence the value of $Accu_{Colour}$ is 1
- Criterion 3 was communicated clearly. Hence the value of $Accu_{Memory}$ is 1
- Criterion 4 was communicated clearly. Hence the value of $Accu_{Model}$ is 1
- Criterion 5 was communicated clearly. Hence the value of $Accu_{Box}$ is 1
- Criterion 6 was NOT communicated clearly. Alice did not specify exactly how the cosmetic condition should be. Hence the value of $Accu_{Condition}$ is 0

Now finding out the significance of each criterion according to Alice, the values of $Sig_{Criterion}$ are achieved:

- Alice assigned a value of 2 to Sig_{Brand}
- A value of 2 to Sig_{Colour}
- A Value of 2 to Sig_{Memory}
- A Value of 1 to Sig_{Model}
- A Value of 1 to Sig_{Box}
- A value of 2 to $Sig_{Condition}$

Now in order to find the $Com_{Interaction}$ for the whole interaction the individual commitment of the all the criterions should be added.

Hence $Com_{Interaction}$ =

$$((Com_{Brand} * Accu_{Brand} * Sig_{Brand}) + (Com_{Colour} * Accu_{Colour} * Sig_{Colour}) + (Com_{Memory} * Accu_{Memory} * Sig_{Memory}) + (Com_{Model} * Accu_{Model} * Sig_{Model}) + (Com_{Box} * Accu_{Box} * Sig_{Box}) + (Com_{Condition} * Accu_{Condition} * Sig_{Condition}))$$

Substituting the respective values in the above equation:

$$Com_{Interaction} = ((1*1*2) + (0*1*2) + (1*1*2) + (1*1*1) + (0*1*1) + (0*0*2))$$

$$\mathbf{Com_{Interaction} = 5}$$

To ascertain the Risk involved in dealing with the trusted peer, the trusting peer needs to find out how much did the commitment of the trusted peer deviated from the promised commitment. For that it needs to find the best possible behavior ($ProCom_{Interaction}$) which also shows the best possible commitment that could have been possible in the interaction.

The best possible commitment in an interaction ($ProCom_{Interaction}$) would have been possible if the trusted peer had acted according to the expected behavior throughout the interaction. That value for the best possible commitment can be achieved by substituting the value of 1 in the place of $Com_{Criterion}$ in equation 1 which shows that all the criterions are satisfied by the trusted peer in the interaction according to the expected behavior.

Hence now finding out the best possible commitment in the interaction ($ProCom_{Interaction}$)

$$ProCom_{Interaction} = ((ProCom_{Brand} * Accu_{Brand} * Sig_{Brand}) + (ProCom_{Colour} * Accu_{Colour} * Sig_{Colour}) + (ProCom_{Memory} * Accu_{Memory} * Sig_{Memory}) + (ProCom_{Model} * Accu_{Model} * Sig_{Model}) + (ProCom_{Box} * Accu_{Box} * Sig_{Box}) + (ProCom_{Condition} * Accu_{Condition} * Sig_{Condition}))$$

Substituting the respective values in the equation we get:

$$ProCom_{Interaction} = ((1*1*2) + (1*1*2) + (1*1*2) + (1*1*1) + (1*1*1) + (1*0*2))$$

$$\mathbf{ProCom_{Interaction} = 8}$$

Substituting the above values of $Com_{Iteraction}$ and $ProCom_{Interaction}$ in equation 2 to find out the Risk involved in the interaction, we get

$$Risk_{Interaction} = 5/8$$

$$Risk_{Interaction} = 0.625$$

Mapping the Risk involved in the interaction to the Riskiness scale by using equation 3 to find out the Riskiness of the trusted peer we get:

$$\text{Riskiness Value} = 0.625 * 5$$

$$\text{Riskiness Value} = \text{ROUND}(3.125)$$

$$\text{Riskiness Value} = 3$$

Hence according to the Riskiness scale Bob is: *Largely Un-Risky,* which complements the fact that he committed to the expected behavior most of the time in the interaction. This level defines neutral risk.

XII. CONCLUSION

In this paper we define the term Riskiness in the context of Peer-to-Peer communications. We then define a Riskiness scale and the individual levels of that scale. Additionally we gave the semantics of what each of the level means.

We then proposed and defined the CCAS metrics that can be used by the trusting peer in determining the Risk during an interaction and assigning a Riskiness value to the trusted peer after the interaction. We then proposed a framework which uses these metrics to assign a Riskiness value to the trusted peer, and explained the framework by using an example.

XIII. REFERENCES

[1]. A. Oram (2001) Peer-to-Peer: Harnessing the Power of Disruptive Technologies Retrieved 16 February, 2004, from http://www.oreilly.com/catalog/peertopeer/chapter/ch01.html.

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

[3]. D. Gefen, V.S. Rao, and N. Tractinsky, 'The conceptualization of trust and their relationship in electronic commerce: The need for clarification', *Proceedings of the 36th Hawaii International Conference on System Sciences,* January 6-9 2003, pp 192-201.

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

[5]. N. Luhmann, 'Familiarity, confidence, trust: Problems and alternatives', *Making and Breaking Cooperative Relations,* Basil Blackwell, New York, USA, 1988.

[6]. R.C. Mayer, J.H. Davis, and F.D. Schoorman, 'An interactive model for organizational trust', *Academy of Management Review*, vol. 20, no. 3, 1995, pp.709-734.

[7]. D.M. Rousseau, S.B. Sitkin, R.S. Burt, and C. Camerer, 'Not so different after all: A cross-discipline view of trust', *Academy of Management Review*, vol. 23, no. 3, 1998, pp. 391-404

[8] P. Sztompka, 'Trust: A sociological theory', Cambridge University Press, Cambridge, U.K, 1999.

[9] S. Grazioli, and A. Wang, 'Looking without seeing: Understanding unsophisticated consumers success and failure to detect Internet deception', *Proceedings of the International Conference on Information Systems, ICIS 2001*, New Orleans, USA, pp 193-204.

[10]. C. Cheung, and M.K.O. Lee, 'Trust in Internet shopping: A proposed model and measurement instrument', *Proceedings of the 6th Americans Conference on Information Systems*, August 10-13 2000, pp 681-689.

[11] K.J. Stewart, 'Transference as a means of building trust in World Wide Web sites', *Proceedings of the International Conference on Information Systems, ICIS 1999*, Charlotte, USA

[12]. S.L. Jarvenpaa, N. Trctinsky, and M. Vitale, 'Consumer trust in an Internet store: A Cross Cultural Validation', *Journal of Computer Mediated Communication,* vol. 5, no. 2, 1999, pp 1-35

[13]. O.K. Hussain, E. Chang, B. Soh, F.K. Hussain, T.S. Dillon, (2005), Factors of Risk Variance in Decentralized Communications, *European Institute of Computer Antivirus Research,* Malta, 30April-3 May 2005, pp 162-170.

[14]. F.K. Hussain, E. Chang, and T.S Dillon, 'Classification of trust in peer-to-peer (P2P) communication', *International Journal of Computer Science and Engineering, vol. 19, no. 2,* 2004.