

# A Methodology for Risk Measurement in e-Transactions

Omar Khadeer Hussain, Elizabeth Chang, *Senior Member, IEEE*, Farookh Khadeer Hussain and Tharam S. Dillon, *Fellow, IEEE*

**Abstract**— Risk is present in almost every activity. Alternately speaking, almost every activity may have some undesired outcomes which the person doing the activity hopes that they do not occur when it undertakes that particular activity. The quantification of those undesired outcomes can be termed as *Risk*. Risk is associated with Trust, Security and Privacy. Risk is also associated with transactions, businesses, information systems, environments, networks, partnerships, etc. Generally speaking, Risk signifies the likelihood of financial loss, human casualties, business destruction and environmental damages. It is important to define Risk according to the context of the transaction in order to understand and analyze it better. In the literature Risk has been defined and discussed in areas such as security, health, finance, environment and social life, but there is no systematic study of Risk in decentralized communications, which involves e-business, computer networks and service oriented environments. Hence in this paper, a particular attention is given to define and analyze Risk in the area of Peer-to-Peer business communications, where Risk is every individual and organization's concern. Also in this paper we develop a risk indicator scale and develop a methodology by which the *Riskiness* of the peer can be rated according to its behavior in an interaction. Risk indicator gives an early warning to the party involved and helps avoid disasters.

**Index Terms**— Criterion, Decentralized Peer-to-Peer Communications, e-Business, Interaction, Risk, Riskiness, Transaction.

## I. INTRODUCTION

Risk is defined in different ways according to the context in which it is being discussed. Each transaction is associated with some kind of Risk and hence it should be defined in accordance to the specific context of the transaction, in order to analyze the correct level of Risk associated with it. The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:2004 too states that Risk Identification is the heart of Risk Management. Hence Risk should be identified according to the context of the transaction in order to

analyze and manage it better. Risk analysis is the science of evaluating health, environmental, and engineering Risks resulting from past, current, anticipated or future activities. The use of these evaluations include providing information for determining regulatory actions to limit Risk, presenting scientific evidence in legal settings, evaluating products and potential liabilities within private organizations, and for educating the public concerning particular Risk issues. Risk analysis is an interdisciplinary science that relies on epidemiology and laboratory studies, collection and exposure of field data, computer modeling, and related social economic and communication considerations. Risk analysis in the area of evaluating health, environmental and engineering activities have different methods for the interpretation and analysis of Risk, and hence consist of specific context based definitions for defining Risk. Unfortunately these methods will not give us a measurable or an accurate answer when they are applied to determine *Risk* in the area of e-commerce and Peer-to-Peer business.

As each transaction is associated with some kind of Risk, it needs to be defined in accordance to that specific context of the transaction, in order to analyze and understand the correct amount of Risk associated. In almost all cases, the amount of Risk involved in a transaction is important to be understood or analyzed before a transaction is begun. This applies to the transactions in the field of e-commerce and Peer-to-Peer business too. One major distinction between the transactions conducted in an e-commerce Peer-to-Peer business environment and other areas is that the latter may consist of physical environments or face to face transaction environments whereas the former area may involve virtual environments [1]. The major difference between the two is that in a physical environment, an idea of the Risk involved in a transaction can be achieved by various physical, facial cues or documents where as for a transaction in the virtual environments there is an absence of such physical cues and hence it is difficult to analyze the Risk involved in these transactions. This scenario is further compounded in e-commerce transactions over the internet and decentralized transactions where the peers dealing with each other may be anonymous. Therefore, what is needed is a mechanism by which we can analyze the Risk involved in dealing with a particular peer particularly in decentralized transactions.

In this paper, our main focus is to first define *Risk* in decentralized transactions and in the area of trusted communications and e-Business. We then focus on defining

Manuscript received October 1, 2005.

Omar Khadeer Hussain is with Curtin University of Technology, GPO Box U1987, Perth WA 6845 (phone: +61-8-92662861; e-mail: Omar.Hussain@cbs.curtin.edu.au).

Elizabeth Chang is with Curtin University of Technology, GPO Box U 1987, Perth, WA 6845 (e-mail: Elizabeth.Chang@cbs.curtin.edu.au).

Farookh Khadeer Hussain is with Curtin University of Technology, GPO Box U1987, Perth, WA 6845 (e-mail: Farookh.Hussain@cbs.curtin.edu.au)

Tharam S. Dillon is with University of Technology, Sydney, Broadway, NSW 2001 (e-mail: tharam@it.uts.edu.au)

a risk indicator and developing a methodology for risk measurement in a transaction.

This paper is organized into XIV sections. Section II discusses about Risk in the literature and the need to analyze Risk in peer-to-peer decentralized transactions. In Section III we define Risk in trusted de-centralized transactions. In Section IV - VI we define the term *Riskiness*, propose and explain the different levels of the Riskiness scale. We then define the criteria of assigning a Riskiness value to a peer in section VII. In section VIII define a standard format for giving recommendation. In section IX – XII we define the metrics used for assigning a Riskiness value to a peer, the levels in each of those metrics and the methodology of assigning Riskiness value to the peer. In section XIII we explain the process of determining Riskiness by using an example. Finally in section XIV we conclude the paper.

## II. STUDYING THE DEFINITIONS OF RISK IN LITERATURE AND NEED TO ANALYZE RISK IN PEER-TO-PEER TRANSACTIONS

*Security* in the virtual world usually refers to the process of enabling sheltered communication between two communicating peers [2]-[4]. *Risk* is defined as the likelihood that the transaction might not proceed as expected in a given context and at a particular time once it begins [5]. The study of Risk can not be compared to the study of Security because securing a transaction does not mean that there will be no Risk to personal damages and financial losses. Risk can be seen as a combination of:

- a) The uncertainty of the outcome and
- b) The cost of the outcomes when it occurs, usually the loss incurred, which is related to Risk.

Risk has been defined in different ways by different researchers. March et al, define Risk more by the magnitude of the value of the outcome rather than by taking its likelihood [6]. This paradigm of Risk is more common in business transactions. Luhmann defines Risk in a transaction where the possible damage might be more than the advantage sought [7]. This type of perception is more common in finance and investments where the expected returns are high. Mayer et al conclude that Risk is present in the transaction only if the negative outcome outweighs the positive outcome at the end of the transaction [8]. In contrast to this definition, Rousseau et al measure Risk as the potential negative consequence and probability of failure [9]. Sztompka defines Risk as the probability of the loss of the resources invested [10]. This is a more general definition of Risk which can be applied to every transaction in any field. Grazioli et al views Risk as the consumer's perception of the uncertainty and adverse consequences of engaging in an activity [11]. Cheung et al define Risk as having two dimensions; one related to the uncertainty or probability of loss notion and the other related to a consequence of the importance of the notion of loss [12]. Stewart classifies Risk as Channel Risk and Store Risk. Channel Risk is also referred to as Internet and Web Risk [13]. The understanding of Internet Risk usually has a significant effect on the willingness of the consumer to buy beyond any effect of the perceived Store Risk. Jarvenpaa define Risk in Information Systems by using items

reflecting its likelihood such as too much uncertainty, how to characterize a decision to proceed with a transaction [14]. Additionally, social dimensions of Risk are addressed by social scientists [15].

The advent of the Internet and its development has simplified the way transactions are carried out. It currently provides the user with numerous facilities which facilitate transaction process. This process evolved into what became known as e-commerce transactions. There are two types of architecture through which e-commerce transactions can be conducted, and they are:

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

In Client-Server architectures servers are powerful computers or processes that specifically manage clients and network traffic. Clients are PCs or workstations on which users run applications and provide an interface to the users. Clients rely on servers for resources, such as information to display, the ability to process the user's request. All the transactions between the clients or the users are passed through the server which checks for its correctness [16].

The second type of architecture is Peer-to-Peer architecture. It is so called because each node has equivalent responsibilities [17, 18]. 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. Some of the characteristics of Peer-to-Peer or decentralized transactions are:

1. There is no server in this transaction between Peers.
2. Peers interact with each other directly, and the interactions are passed to them, rather than through a server as compared to a centralized transaction.
3. 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.

The above properties clearly show that a decentralized transaction carries more Risks and hence merits more detailed investigations. Decentralized or Peer-to-Peer transactions can be compared with distance transactions that have much in common with catalogue mail ordering systems. 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. The consumer generally has no opportunity to see and try the product before buying it. Thus this shows that 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 [15]. 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 usually does not tend to act as a medium to buy, but as a means for providing information. The likelihood of a negative outcome might be the same in both the high cost and the low cost 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, as compared to the demand for lower cost items, would be consistent with the idea that the 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 transactions are being described as the next generation of the Internet [19]. Architectures have been proposed by researchers for integrating web services with peer-to-peer communicating agents like Gnutella [20]-[23]. However, Peer-to-Peer transactions suffer from some disadvantages and Risk in the transaction is one of them. Hence we need to develop a mechanism by which we can overcome this disadvantage so that they can be used effectively with whatever service they are being integrated with.

There is still confusion in the relationship between Trust and Risk. As Mayer et al suggest 'it is unclear whether Risk is an antecedent to trust' [8]. As discussed in Hussain et al [24] 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. Different arguments can be given to this statement. It can be said that in an interaction Risk creates an opportunity for Trust which leads to Risk taking [27]. 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. Some methodologies have been proposed to establish trust in an interaction [25]-[26]. Risk can also 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 Trust and Risk are two different components that complement each other [27]. The higher the Trust, the lower the Risk will be and vice versa. Trust signifies the belief that one peer has in another peer where as Risk signifies the consequences to a peer resulting from engaging in an activity with another peer. Consequences refer to the loss in the interaction, whether it is financial or any other loss.

As mentioned earlier, the inclusion of Risk in the study of behavior in e-commerce transaction is important because there is a large volume of literature based in rational economics that argues that the decision to proceed with the transaction is based on the Risk adjusted cost benefit analysis. Hence analyzing Risk 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 [28].

Through the above discussion, it is evident that Risk measurement is indeed needed in electronic commerce and Peer-to-Peer business. We need a Risk management tool that follows and complies with the Australian and New Zealand Standard on Risk Management AS/NZS 4360:2004, that helps in analyzing, evaluating and treating the Risk [29]. In the literature we note that Risk has not been defined by taking the context of Peer-to-Peer transactions into consideration nor there is such a methodology defined to measure Risk.

Keeping this in mind, we propose the definition of Risk involved during a decentralized transaction in e-commerce in the next section. We also propose a methodology for measuring Risk in an interaction in the next sections.

### III. DEFINING RISK IN TRUSTED DE-CENTRALIZED TRANSACTIONS

We define **Risk** between two peers in a P2P interaction as the *likelihood* that the *trusted peer* might *not act as expected* according to the *trusting peer's* expectations in a given *context* and at a *particular time* once the interaction begins, resulting in the loss of \$ and the resources involved in the interaction.

The terms in underlined italics are important and form the building blocks for defining risk in decentralized transactions. We will explain what these terms mean in the next sub-section through an example.

#### A. *Trusting Peer*

As described in Hussain, Chang and Dillon [30], *trusting peer* is the entity who controls the resources and who has to repose his faith in the other entity, if he plans to deal with him.

For example, let us consider a scenario of an interaction between John and Mary. John wants to buy an MP3 player from Mary, it is John who has the resources and who is going to repose his faith in Mary for the interaction to begin. Hence, John is the Trusting Peer in this case.

#### B. *Trusted Peer*

As also described in Hussain et al [30], *trusted peer* is the entity with whom the trusting peer deals with and reposes faith in.

Considering the above example, Mary is the *Trusted Peer* as she is the entity with whom John, the trusting peer deals with after reposing his faith in her.

#### C. *Not Act As Expected*

Before starting an interaction, the trusting peer sets its criteria of the interaction to the trusted peer. In order for the successful completion of the interaction, the trusted peer should behave in such a way that it fulfills each criterion of the interaction. This behavior of the trusted peer is termed as *expected behavior*, or when both the peers agree to behave in a certain way then it is known as *mutually agreed behavior* [30].

When the trusted peer deviates or fails to perform according to the expected behavior or mutually agreed behavior then it can be termed as *not act as expected*.

For example, John and Mary come to a conclusion that the MP3 player should be sent to the buyer as soon as the money is received by the seller. This is the criteria or the mutually agreed behavior. But suppose that Mary delays in sending the MP3 player to John after receiving the money from him, then she is not acting as John expected or as mutually agreed. This is termed as *not act as expected*.

#### D. Likelihood

*Likelihood* refers to possibility, or to an allusion which is not clearly understood or too readily predicted. An allusion or doubt comes in mind, when we want a certain thing to happen, but are not sure of what the outcome is going to be. When an interaction is proceeding in a direction in which we do not want it to, then there is likelihood of its unsuccessful completion, which can be termed as *Risk*.

Extending the above example, when Mary does not send the MP3 player to John as she was supposed to after the payment is received, then there is likelihood that she will not respond to him as expected and complete the interaction as expected.

#### E. Context

*Context* is defined as the purpose for which the interaction is being held. When discussing about Risk, it is important to take context into consideration, as Risk can be dynamic and might not be the same for each context. When we are speaking of Risk in an interaction between two peers, we take into consideration only that particular interaction in the particular context, and not any other interaction between those two peers in any other context.

Explaining with an example, the above interaction between Mary and John is for an MP3 player. Hence, the *context* for the above interaction is provision of an MP3 player. The risk we are discussing between John and Mary in this scenario is over the dealing of a MP3 player.

Suppose that Mary and John deal again some time over a different thing, such as a computer. The context of this interaction is the computer. The Risk that was between John and Mary in the interaction of the MP3 player might not be the same in the interaction of the computer as this is a different context.

When we are taking into consideration the context of the interaction it doesn't mean that it covers the whole context. Even in the same context, different trusting peers might have different criteria for the assessing the completeness of the interaction. This is further explained in section VII.

#### F. Particular Time

*Time* too is important while determining Risk. Risk is dynamic and it is not possible for the trusting peer to have the same impression of a trusted peer throughout, which it had at a particular time. The impression for the trusted peer by the trusting peer can either improve or degrade as the interaction progresses, scaling the Risk associated with the interaction along with it.

For example, let us consider the scenario before John starts an interaction of the MP3 player with Mary. He has

not interacted with Mary before and hence the Risk in the interaction might be high. But as the interaction progresses and if Mary completes the criteria of the interaction according to the expected behavior, then John might get a better idea of the willingness and capability of Mary, scaling the Risk accordingly with the impression achieved. When we are speaking of Risk at a particular time, we are capturing the dynamic nature of Risk associated with the interaction at that particular instant.

As discussed in the previous section, in a decentralized transaction the peers deal with each other either face-to-face or over the Internet without knowing each other. Before starting an interaction, if they can know about the nature of the trusted peer then it will assist them greatly in making a decision to proceed with the interaction or not. By the 'nature of the trusted peer' we mean the level of Risk that could be involved in dealing with the peer. In this paper we try and propose such a methodology, by assigning the trusted peer in an interaction 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 a particular peer. In the next section we define what the term *Riskiness* means and then define seven different *Riskiness* levels on the Riskiness scale. Further we define the semantics associated with those levels and propose a methodology by which the trusting peer assigns a *Riskiness* value to the trusted peer after the interaction, depending on the behavior of the trusted peer by using the proposed metrics.

## IV. DEFINING THE TERM RISKINESS

Riskiness is defined as *the numerical value that is assigned by the trusting peer to the trusted peer after the interaction, which shows its level of Risk on the Riskiness scale*.

It also quantifies the range of Risk present in the interaction. 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.

## V. RISKINESS LEVELS AND THEIR SEMANTICS

In this section we define the Riskiness scale and explain its different levels. We also explain the semantics associated with each level and its corresponding Riskiness value.

Figure 1 shows the 7 different levels of Riskiness and their corresponding values 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 trusting peer depending on its behavior in the interaction. This value shows the level of Risk present in dealing with that particular trusted peer. The Riskiness scale has 6 levels to represent each type of Risk and one level to represent Unknown Risk.

## VI. SEMANTICS OF THE RISKINESS LEVELS AND THEIR POSTULATES

In this section we define the different Riskiness levels, their corresponding Riskiness values and the semantics that are associated with each of these Riskiness value. We also

define the postulates for these levels. Postulates define the possible scenario by which the trusted peer might get the particular level and hence its corresponding Riskiness value.

#### A. Unknown Risk

The first level of the Riskiness scale is termed as Unknown Risk and its corresponding Riskiness value is -1. This level suggests that the level of Risk is unknown. A peer assigned with this Riskiness value is termed as an *Unknown Risk peer*.

**Semantics:** This value is assigned to the trusted peer 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 recommending this 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 the peer-to-peer network.
- The recommending peer does not have any previous interaction with the trusted peer and hence is not in a position to recommend the Riskiness of the trusted peer.

#### B. Totally Risky

The second level of the Riskiness scale is defined as Totally Risky. The corresponding Riskiness value of this level is 0. A Riskiness value of 0 suggests that the level of Risk in the interaction is between 90-100%. A peer with the Riskiness value of 0 is termed as a *Totally Risky peer*.

**Semantics:** This level and its corresponding value on the Riskiness scale suggest that at a given point of time and at a given context the trusted peer is totally or completely unreliable to perform a given action. In other terms it 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.

A peer which has been assigned a Riskiness value of 0 is defined as a *Totally 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 is giving the recommendation about the trusted peer,
- The trusted peer did not commit to the expected behavior at all even after the trusting peer had communicated all the factors or bases against which its actual behavior is going to be analyzed.











| Riskiness Levels | Magnitude of Risk  | Riskiness Value | Star Rating   |
|------------------|--------------------|-----------------|---|
| Unknown Risk     | .                  | - 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 different levels of the Riskiness scale and the corresponding range of Riskiness values and the star visual representation.

#### C. Extremely Risky

Extremely Risky is the third level on the Riskiness scale with a Riskiness value of 1. This level denotes that there is 71-90 % of Risk in the interaction. A peer assigned with a Riskiness value of 1 is termed as an *Extremely Risky peer*.

**Semantics:** This level on the Riskiness scale demonstrate that at a given point of time and at a given context the trusted peer is unreliable to a greater extent to perform a given action by seeing its level of un-commitment in the interaction. In other terms it deviates from the expected behavior or mutually agreed behavior most of the times, hence increasing the Risk too accordingly. A Riskiness value of 1 expresses the lesser level of high Risk.

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

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

- The trusted peer deviates from the expected behavior most of the times even after the trusting peer had communicated all the factors or bases against which its Riskiness is going to be analyzed.

#### D. Largely Risky

The fourth level of the Riskiness scale is termed as Largely Risky. The corresponding Riskiness value of this level is 2. This level depicts that there is a Risk of 51-70 % in the interaction. A peer assigned with a Riskiness value of 2 is termed as a *Largely Risky peer*.

**Semantics:** A Riskiness value of 2 signifies a level of medium 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 be regarded as unsatisfactory. A Riskiness value of 2 expresses the lesser level of medium risk.

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

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

- The trusted peer had been communicated MOST or ALL the bases against which it’s Riskiness will be evaluated

and he did not commit in most of the criterions according to the expected behavior.

#### E. Risky

The fifth level on the Riskiness scale is termed as Risky and it is shown by a Riskiness value of 3. This level outlines that there is 26-50 % of Risk in the interaction. A peer with Riskiness value of 3 is termed as a *Risky peer*.

**Semantics:** This level suggest that a peer assigned with a Riskiness value of 3 on the Riskiness scale can be relied upon to complete a task up to a certain extent. Broadly speaking this type of Risk can be termed as medium Risk, but this medium risk leans more to the positive side (Levels 4 & 5). Hence a Riskiness value of 3 expresses the larger level of medium 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).

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

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

- The trusted peer might not have been communicated MOST of the bases against which its Riskiness will be evaluated.

#### F. Largely UnRisky

The sixth level on the Riskiness scale is defined as Largely UnRisky with a corresponding Riskiness value of 4. This level depicts that there is a Risk of 11-25% in the interaction. A peer with a Riskiness value of 4 is termed as a *Largely UnRisky peer*.

**Semantics:** This level on the Riskiness scale suggests that a peer assigned with this value can be relied on to perform a given 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. This level represents the lesser level of low Risk in an interaction.

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

#### G. UnRisky

UnRisky is the seventh and the last level of the Riskiness scale. The Riskiness value used to represent this level is 5. This level shows that there is 0-10 % of Risk in the interaction. A peer assigned with a Riskiness value of 0 is termed as an *Un-Risky peer*.

**Semantics:** This level and its corresponding Riskiness value imply 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 his commitment in the criterions is EXACTLY according to expected behavior or mutually agreed behavior and the interaction is totally safe and hence there is no un-committed behavior. If there is any Risk in this interaction then it will be minimal.

This level defines the absence of Risk in the interaction or if any present then the lowest possible amount of Risk. 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 an *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 commits to all that is expected from the trusting peer for this interaction and there is very less degree of un-committed behavior in the interaction.

## VII. CRITERIA FOR RISK MEASUREMENT

Our method of assigning Riskiness to a peer is by assessing the level of un-committed or un-fulfilled behavior in the interaction with respect to the expected behavior. This is achieved through the notion of *expectations* i.e. the expected behavior, or the Mutually Agreed Behavior and *assessing un-commitment* i.e. assessing to what extent or level the trusted peer did not fulfill or commit to the expected behavior in its actual behavior. In other terms it can be said as the difference between expected behavior and actual behavior, which gives the un-committed behavior. This un-committed behavior is used to measure the Risk in the interaction. The greater the difference between the expected and committed behavior the higher the level of Risk present in the interaction and vice versa.

In other words arriving at a level of risk rating for the trusted peer can be seen as an interaction between the trusting and the trusted peer. The Riskiness value that the trusted peer gets from the trusting peer is dependent on a number of accessing criteria. The accessing criteria are defined as the set of factors or bases against which the un-committed behavior of the trusted peer is going to be determined in the interaction. The accessing criteria are derived from the expected behavior or the mutually agreed behavior. We call the accessing criteria in an interaction as *criteria*. The criteria for determining the Riskiness of a trusted peer in a particular context are not same for each and every interaction. They vary according to each trusting peer. Hence even in the same context, the criteria of two trusting peers for assessing the un-committed behavior of a particular trusted peer might be different. For example suppose that two trusting peers 'B' and 'C' interact with a trusted peer 'A' over the same context. The criteria of each trusting peer for assessing the un-committed behavior of the trusted peer 'A' in the interaction might be different from each other and the Riskiness value they assign to the trusted peer 'A' after their interaction with it, is on its level of un-commitment or un-fulfillment according to the criteria of their interaction.

Hence even in a single interaction the basis for determining the Riskiness of a trusted peer depends on a number of criterions. The sum of the level of fulfillment or

commitment in those criteria by the trusted peer is determined. This is compared with the best possible commitment or the promised commitment that was expected from the trusted peer, knowing the level of un-committed behavior in the interaction. The level of un-committed behavior scaled to the Riskiness scale is the final value which is assigned to the trusted peer as its Riskiness value in the interaction. The trusting peer will assess the level of fulfillment or commitment in the actual behavior by using some metrics. Those metrics are defined in section IX. If the trusting peers expectations are met then a corresponding favorable score to the trusted peer will be assigned by the metrics.

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. After asking for recommendations from the other peers for Bob, Alice decides to proceed in the interaction. So the criteria on which Alice is going to determine the Riskiness of Bob are:

- 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.

In order to assign a Riskiness value to Bob, Alice will first assess the level of commitment in Bob's actual behavior according to these criteria and then compare it with the promised commitment or the expected behavior from Bob, knowing the un-committed behavior in the interaction. She will then map the level of uncommitted behavior to the Riskiness scale, in order to get Bob's Riskiness value in the interaction.

### VIII. SOLICITING RECOMMENDATION FROM OTHER PEERS

If the trusting peer wants to proceed in an interaction with a particular peer and had not interacted with it before in the same context and time slot, then it will ask for recommendations from other peers. It will issue a reputation query to the other peers asking for recommendations about the particular peer specifying the context, time and its criteria. The peers giving recommendations as called as the recommending peers [31]. The recommendation can be given by any peer present on the network. However, it is highly unlikely that the recommendations provided by the peers would be completely reliable. Hence the recommendations can be classified into three categories namely trustworthy, untrustworthy and unknown recommendations. The trusting peer assimilates the recommendations from the trustworthy and unknown peers and ignores those from the untrustworthy peers, as the Risk in accepting those recommendations might be high. The process of classifying the recommendations as trustworthy, unknown and untrustworthy is discussed in Hussain et al [31] and we will not be discussing it in here. Based on these

recommendations the trusting peer can take a decision of proceeding in the interaction with the particular peer or not.

The recommending peers reply back with the Risk Set as their recommendation. The Risk set contains the recommended Riskiness value for the particular peer, as recommended by the recommending peer depending on their last interaction with it. As explained in Hussain et al [32] the Risk set is an ordered way of representing the various details of their last interaction with the particular peer, by the recommending peer, so that the trusting peer asking for recommendations can know the meaning of each element in the recommendation and consider only those recommendations in determining the Riskiness value of the trusted peer whose criteria are of interest to it in its present interaction. The format of the Risk set is:

{TP1, TP2, Context, CR, R', (Assessment Criteria, Commitment level), R, Cost, Start time, End time, RRP}  
Where:

TP1 is the Trusting peer in the interaction. This is also the recommending peer while giving recommendations,

TP2 is the Trusted peer in the interaction,

Context represents the context of the transaction,

CR represents the Current Riskiness value of the trusted peer before the interaction, which is achieved either by the last interaction of the trusting peer with the trusted peer in the same time slot or by asking recommendations from other peers and assimilating those recommendations to determine the Riskiness value of the trusted peer according to the criteria of the trusting peer in the interaction,

R' shows the predicted Riskiness value of the trusted peer depending on its past values,

(Assessment Criteria, Commitment level) shows the factors or bases which the recommending peer used in its interaction with the trusted peer to assign it a Riskiness value. These criteria are necessary to mention while giving recommendations, so that a trusting peer who asks for the recommendation knows the factors or bases on which this particular trusted peer was assigned the recommended Riskiness value and can take only those recommendations which are of interest to it according to the criteria of its interaction. Commitment level specifies whether the particular criterion was fulfilled by the trusted peer or not. A value of either 0 or 1 is assigned here based on the evaluation of the particular criterion measuring for its fulfillment according to the metric Eval<sub>Criterion</sub>. Further explanation is given in the next section,

R is the Riskiness value assigned by the recommending peer to the trusted peer after the interaction,

Cost represents the cost of the transaction,

Start Time is the time at which the recommending peer started the transaction with the trusted peer,

End time is the time at which the transaction of the recommending peer ended with the trusted peer,

RRP is the Riskiness value of the recommending peer while giving recommendations. This value is used to determine whether recommendation is trustworthy or not.

## IX. METRICS FOR ASSIGNING A RISKINESS VALUE TO A TRUSTED PEER

As mentioned in section VII, our method of assigning Riskiness to a peer is by assessing the level of un-committed behavior in the interaction with respect to the expected behavior. This is achieved through the notion of *expectations* and *assessing un-commitment* in those expectations.

By *Expectations* we mean the expected behavior. This is the way in which the interaction is supposed to proceed [30] according to the criteria of the interaction. *Expectations* also refer to mutually agreed behavior that is the promised commitment from the trusted peer.

By *Assessing Un-commitment* we mean assessing the degree of un-fulfillment or un-commitment in the actual behavior of the trusted peer with respect to the expected behavior of an interaction. To achieve that we will first determine the level of commitment that the trusted peer showed in its behavior in the interaction. This will depict how the trusted peer actually behaved in the interaction and how much did he fulfill according to the expected behavior. If the level of commitment i.e. the actual behavior is compared with the expected behavior i.e. the promised commitment, then the un-committed behavior in the interaction can be determined.

In this section we will define the metrics for assessing the level of commitment by the trusted peer based on its actual behavior in the interaction.

### A. Metric 1: Assessment of an Interaction ( $Asses_{Interaction}$ )

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

- Evaluating the level of fulfillment in the behavior of the trusted peer in each criterion of an interaction.
- Adding up the evaluations of all the criterions to get the total assessment of the interaction ( $Asses_{Interaction}$ ).

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 assess the level of fulfillment or commitment by Bob by determining:

- 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 assessment of fulfillment in the interaction will be ascertained by evaluating the fulfillment of each criterion. We represent the evaluation of fulfillment of each criterion as  $Eval_{Criterion}$ .

Therefore the assessment of fulfillment of the interaction in this case can be found out by

- Evaluating the level of fulfillment in the behavior of Bob in selling the MP3 player of the specific model to Alice which she wants ( $Eval_{Model}$ )

- Evaluating the level of fulfillment in the behavior of Bob in selling the MP3 player of the same colour to Alice which she wants ( $Eval_{Colour}$ )

Therefore evaluation 1 = *model*, evaluation 2 = *colour*. These two individual values show the evaluation of fulfillment in each criterion. The total assessment of the interaction can be found out by adding the evaluation of each criterion, i.e.  $Eval_{Model} + Eval_{Colour}$ .

Hence the total assessment of fulfillment in an interaction can be found out by adding the individual evaluation of each criterion.

$$Asses_{Interaction} = \sum_{i=1}^n (Eval_{Criterion\ i})$$

Where n is the number of criterions in an interaction.

### B. Metric 2: Evaluation of a Criterion ( $Eval_{Criterion}$ )

$Eval_{Criterion}$  is measured as evaluating the degree of fulfillment in the actual behavior of the trusted peer with respect to the expected behavior of the trusting peer in a criterion. In the end the evaluation of a criterion ( $Eval_{Criterion}$ ) should be a numeric value. That is achieved by mapping the degree of fulfillment of a criterion to its corresponding level, which in turn shows whether the trusted peer committed in the criterion as expected by the trusting peer or not.

Considering the above example of the interaction between Bob and Alice, the evaluation of the criterions ( $Eval_{Model}$  and  $Eval_{Colour}$ ) can be done 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 evaluate the degree of fulfillment in the actual behavior with respect to the expected behavior we define two levels of  $Eval_{Criterion}$ . Those levels are explained in the next section.

As explained earlier while evaluating the fulfillment 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.

### C. Metric 3: Familiarity of the Criterion ( $Fam_{Criterion}$ )

The metric  $Fam_{Criterion}$  takes into account the familiarity of the trusted peer with a particular criterion when determining its Riskiness value. As mentioned before, the trusting peer will take the recommendation of other peers if it has not interacted with the trusted peer before in the same context and time slot. Based on the those recommendations or based on the previous interaction of the trusting peer with the trusted peer in the same time slot, a value is assigned to the metric  $Fam_{Criterion}$  which shows the familiarity of the trusted peer with the particular criterion. This is taken into account while determining its Riskiness value.

To explain with an example let us suppose that Alice has not interacted with Bob before and asks for its recommendations from other peers in the context of buying an MP3 player. A recommending peer 'C' replies back



giving its recommendation to Alice in the form of Risk set as explained in the previous section. From the recommendation Alice notes that the criteria in her interaction are same as those of the recommending peer 'C', and in that Bob had fulfilled all of the criteria according to the expected behavior. Hence based on the recommendation Alice proceeds in the interaction with Bob, as he is familiar before with the criterions that Alice wants in her interaction. But during the interaction with Alice, Bob does not commit totally in its behavior to the criterions. Hence Bob deserves a Riskiness value lower on the Riskiness scale as compared to what he would have deserved if he wasn't familiar with the criterions before. In spite of being familiar with the criterions before in its previous experience, he did not fulfill it in this particular interaction. The Risk in dealing with Bob is high as compared to any other peer who wasn't familiar with the criterions before. Hence Bob warrants a Riskiness value correspondingly. The metric  $Fam_{Criterion}$  takes into account the previous familiarity of the trusted peer with the particular criterion according to the recommendations or previous interactions while determining the Riskiness value.

We will define the different levels that show whether the trusted peer was familiar with the criterions or not in the next section.

#### D. Metric 4: Accuracy of the Criterion Communication ( $Accu_{Criterion}$ )

Riskiness can be correctly analyzed when the trusted peer knows all the factors and bases against which the criterion is going to 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 discussed before 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 fulfillment of a criterion were communicated clearly to the trusted peer or not in the next section. This will be taken into consideration while assessing the fulfillment of an individual criterion.

#### E. Metric 5: Significance of the Criterion ( $Sig_{Criterion}$ )

Another important factor to consider while assessing the fulfillment of an interaction is the Significance of each criterion. We define the metric  $Sig_{Criterion}$  which expresses the significance of the 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 according to the trusting peer.

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 sends the MP3 player of the specific model which Alice wants.
- Whether the MP3 player is of the same colour which Alice wants.
- Whether Bob sends 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 more on the first two factors in assessing the level of fulfillment in the actual behavior with respect to the expected behavior to determine the Riskiness value.

Similarly for explanation sake 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 equally while assigning a 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.

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

## X. LEVELS FOR THE METRICS DEFINED

In this section we propose the levels for the metrics defined in the previous section, namely  $Eval_{Criterion}$ ,  $Fam_{Criterion}$ ,  $Accu_{Criterion}$  and  $Sig_{Criterion}$ . Using these values of the respective levels we will derive the value of  $Asses_{Interaction}$  in the next section.

### A. Levels of $Eval_{Criterion}$

In order to assign a correct Riskiness value to the trusted peer, the trusting peer will need to evaluate whether a particular criterion has been fulfilled in accordance with the expected behavior. For that we define two levels for  $Eval_{Criterion}$ . 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 1.

**B. Levels for Fam Criterion**

In order to consider the familiarity of the trusted peer with the particular criterion, while determining its Riskiness value we define two levels of Fam Criterion. These levels show whether the trusted peer was familiar with the particular criterion or not. The numerical value which corresponds to the level of familiarity should be taken in consideration while determining the Riskiness value. The levels are shown in table 2.

**C. 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 will be used to judge the behavior of the trusted peer in the particular criterion have been communicated to it in clear terms. So in order to determine the accuracy by which the factors were 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 criterion was defined will be taken into consideration, while determining the Riskiness of the trusted peer. The levels are explained in table 3.

**D. 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 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 determining the Riskiness of the trusted peer. So in order to assign a significance value to the criterion we define two levels for the metric Sig Criterion. Those levels are explained in table 4.

**XI. ASSESSING THE COMMITMENT IN THE WHOLE INTERACTION (ASSES INTERACTION)**

Once a value from each metric defined in the previous section has been assigned to all the criterions, then the total assessment of commitment by the trusted peer in the interaction can be determined. As explained before the total

TABLE 1  
SHOWING THE LEVELS FOR THE METRIC EVAL CRITERION

| Eval Criterion Value | Semantics of the Value   |
|----------------------|--|
| 0                    | The trusted peer did not fulfill the criterion as it was expected from him according to the expected behavior or as it was promised according to the mutually agreed behavior. |
| 1                    | The criterion was fulfilled exactly according to the expected behavior, i.e. there is no deviation between the actual behavior and the expected behavior.                      |

TABLE 2

SHOWING THE LEVELS FOR THE METRIC FAM CRITERION

| Fam Criterion Value | Semantics of the Value   |
|---------------------|--|
| 1                   | According to the recommendations or the previous interaction of the trusting peer with the trusted peer, the trusted peer is NOT familiar with the particular criterion. |
| 2                   | The trusted peer is familiar with the particular criterion and has experience of it in its past interactions.  |

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   |
|---------------------|--|
| 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.   |

assessment of commitment in the interaction Asses Interaction will take into consideration:

- The criteria against which the assessment is going to be determined,
- Evaluating the level of fulfillment in each of the criterion Eval Criterion,
- The familiarity of the trusted peer with those criterions Fam Criterion,
- The accuracy by which those criterions were communicated to the trusted peer Accu Criterion ,
- The Significance of each criterion Sig Criterion.

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

$$\text{Asses}_{\text{Interaction}} = \sum_{i=1}^n ((\text{Eval}_{\text{Criterion } i} * \text{Fam}_{\text{Criterion } i}) * \text{Accu}_{\text{Criterion } i} * \text{Sig}_{\text{Criterion } i})$$

where  $i$  represent a particular criterion and  $n$  represents the number of criterions in the interaction. The above equation indicates that the assessment of fulfillment in an interaction  $\text{Asses}_{\text{Interaction}}$  is:

- The sum of evaluations of each criterion in an interaction.
- And each criterion is further evaluated based on its familiarity, accuracy and significance.

So if there are three criterions in an interaction the assessment of the interaction ( $\text{Asses}_{\text{Interaction}}$ ) which shows the level of fulfillment in the actual behavior of the trusted peer can be calculated as:

$$\begin{aligned} \text{Asses}_{\text{Interaction}} = & \\ & (((\text{Eval}_{\text{Criterion } 1} * \text{Fam}_{\text{Criterion } 1}) * \text{Accu}_{\text{Criterion } 1} * \text{Sig}_{\text{Criterion } 1}) + \\ & ((\text{Eval}_{\text{Criterion } 2} * \text{Fam}_{\text{Criterion } 2}) * \text{Accu}_{\text{Criterion } 2} * \text{Sig}_{\text{Criterion } 2}) + \\ & ((\text{Eval}_{\text{Criterion } 3} * \text{Fam}_{\text{Criterion } 3}) * \text{Accu}_{\text{Criterion } 3} * \text{Sig}_{\text{Criterion } 3})) \end{aligned}$$

**Equation----- 1**

## XII. DETERMINING THE UN-COMMITTED BEHAVIOR IN THE INTERACTION

To find out the Riskiness of the trusted peer, the trusting peer after finding out the level of commitment in the trusted peer's actual behavior will need to determine how much this committed behavior is far from the best possible behavior. The difference between those two behaviors gives the level of un-committed behavior in the interaction by the trusted peer.

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 peer makes before the interaction. We represent it as  $\text{ProCom}_{\text{Interaction}}$  which shows a numerical value that quantifies the maximum possible commitment that could have happened in an interaction, if the trusted peer had acted according to the expected behavior.

The value that the trusting peer gets for  $\text{Asses}_{\text{Interaction}}$  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  $\text{Asses}_{\text{Interaction}}$  and vice versa. So in other terms  $\text{Asses}_{\text{Interaction}}$  depicts how the trusted peer behaved in the interaction i.e. the actual behavior.

We define  $\text{Risk}_{\text{Interaction}}$  as the metric which expresses the Risk in the interaction. This is achieved by expressing the level of un-commitment in the interaction with respect to the promised commitment. The level of un-commitment in the interaction is found by the difference between the promised

commitment ( $\text{ProCom}_{\text{Interaction}}$ ) i.e. the numerical value which quantifies the expected behavior and the level of fulfillment or commitment in the interaction by the trusted peer ( $\text{Asses}_{\text{Interaction}}$ ) i.e. the numerical value which quantifies the actual behavior.

Hence  $\text{Risk}_{\text{Interaction}}$  is expressed as

$$\text{Risk}_{\text{Interaction}} = \frac{\text{ProCom}_{\text{Interaction}} - \text{Asses}_{\text{Interaction}}}{\text{ProCom}_{\text{Interaction}}}$$

**Equation ----- 2**

$$\text{Percent of Risk}_{\text{Interaction}} = (\text{Risk}_{\text{Interaction}} * 100)$$

**Equation-----3**

In other terms Percent of  $\text{Risk}_{\text{Interaction}}$  shows the percent of Risk that was there in the interaction between the trusting peer and the trusted peer. It also shows the extent to which the trusted peer did not fulfilled or commit 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). Each level on the Riskiness scale defines a degree of Risk present in the interaction as explained in section V. The trusting peer should map the percent of Risk in the interaction to the Riskiness scale. The percent of Risk in the interaction depicts the percentage of un-committed behavior in the interaction with respect to the promised commitment. The level which corresponds to the percent of Risk in the interaction on the Riskiness scale is the Riskiness level of the trusted peer and its corresponding value is the Riskiness value of the trusted peer. Hence the Riskiness value of the trusted peer is

Riskiness value of the trusted peer =

$$\text{LEVEL} (\text{Percent of Risk}_{\text{Interaction}})$$

**Equation----- 4**

This can also be written as:

$$\text{Riskiness Value} = \text{LEVEL} \left( 1 - \frac{\text{Asses}_{\text{Interaction}}}{\text{ProCom}_{\text{Interaction}}} * 100 \right)$$

Or alternately speaking

Riskiness Value =

$$\text{LEVEL} \left( 1 - \sum_{i=1}^n \frac{((\text{Eval}_{\text{Criterion } i} * \text{Fam}_{\text{Criterion } i}) * \text{Accu}_{\text{Criterion } i} * \text{Sig}_{\text{Criterion } i})}{((\text{ProCom}_{\text{Criterion } i} * \text{Fam}_{\text{Criterion } i}) * \text{Accu}_{\text{Criterion } i} * \text{Sig}_{\text{Criterion } i})} * 100 \right)$$

where  $n$  represents the number of criterions in the 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.

### XIII. EXAMPLE FOR DETERMINING THE RISKINESS VALUE OF A PEER BY USING THESE METRICS

In this section we will explain the process of finding the Riskiness of a trusted peer on the Riskiness scale by using the above metrics. To proceed further we will assume the following interaction in which a peer 'A' wants to deal with a logistic company 'X' for transporting its goods from one place to another. Thus peer 'A' is the trusting peer in this interaction in the context of transporting its goods and peer 'X' is the trusted peer.

Peer 'A' and the logistic company 'X' 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 which is also the criteria of the interaction. The criteria of peer 'A' in the interaction are:

1. Packing the goods properly,
2. Pick up of the goods on time,
3. Delivery of the goods to the destination address on time,
4. Unpacking the goods at the destination address ,
5. Delivering the goods in the same condition as pick up,
6. Providing with a facility of track and trace.

Suppose peer 'A' wants the goods to be unpacked and arranged according to how it wants at the destination address. But he did not communicate it accurately to the trusted peer as seen in criterion 4.

As peer 'A' has not interacted with the logistic company 'X' before, it asks for recommendation from other peers which had previously interacted with the logistic company 'X', by specifying its context. Let us suppose that it gets recommendation from 3 peers, peer 'B', peer 'C' and peer 'D'. They are called as the recommending peers. As explained in section VIII the recommendation that the recommending peers give need not be trustworthy always. They can either be trustworthy, untrustworthy or unknown. The trusting peer takes only the trustworthy and unknown recommendations into consideration, and further assimilates those recommendations according to the criteria of its interaction to determine the recommended Riskiness value of the trusted peer, hence leaving out the untrustworthy recommendations. The process of determining whether the recommending peer is giving trustworthy or un-trustworthy recommendation and further assimilating the trustworthy and unknown recommendations according to the criteria of the trusting peer's interaction is discussed in Hussain et al [31] and we will not be discussing it in here. But for explanation sake and continuing with the above example let us assume its concept that a recommending peer whose Riskiness value while giving recommendations (RRP) is within the range of (-1,1) is said to be giving trustworthy recommendation.

The recommendation given by peer 'B' in the form of Risk set is:

{Peer 'B', Logistic Company 'X', Transporting the goods, 4, 4, ((Pickup of goods, 1) (Delivery of goods, 1)), 4, 1000, 02/08/2005, 09/08/2005, 0.8}

The recommendation given by peer 'C' in the form of Risk set is:

{Peer 'C', Logistic Company 'X', Transportation of goods, 4, 5, ((Packing of goods, 1) (Pickup of goods, 0) (Delivery of goods in same condition, 0) (Unpacking of goods, 1)), 3, 800, 15/08/2005, 22/08/2005, 0.5}

The recommendation given by peer 'D' in the form of Risk set is:

{Peer 'D', Logistic Company 'X', Goods Transportation, 3, 3, ((Pickup of goods, 0) (Delivery of goods, 1)), 2, 200, 5/07/2005, 5/07/2005, 2}

By seeing the Riskiness value while giving recommendation (RRP) for the peers it can be concluded that peer 'B' and peer 'C' are giving trustworthy recommendations and Peer 'D' is giving untrustworthy recommendation. Hence peer 'A' will take the recommendations from peer 'B' and peer 'C' only and leave the recommendation from peer 'D'.

Based on these recommendations peer 'A' decides to proceed in the interaction with the logistic company 'X'. Let us suppose that this was the behavior from the logistic company 'X' in the interaction:

1. Packed the goods properly as promised,
2. Picked up the goods on time as promised,
3. Did not deliver the goods on time,
4. Unpacked the goods at the destination address,
5. Delivered the goods in the same condition,
6. Provided with the facility of track and trace.

This can be termed as the actual behavior in the interaction by the logistic company 'X'.

In order to determine the Riskiness of the logistic company 'X', peer 'A' will first assess the level of fulfillment or commitment in the actual behavior of the logistic company 'X' with respect to the expected behavior in each criterion. So the value of Eval<sub>Criterion</sub> can be determined according to its metric as follows:

- For the first criterion the logistic company 'X' packed the goods properly, and fulfilled the criterion according to the expected behavior. So the value of Eval<sub>Packing</sub> according to table 1 is 1.

- For the second criterion the logistic company 'X' picked up the goods on time. So it fulfilled the criterion according to the expected behavior. Hence the value of Eval<sub>Pickup</sub> is 1.

- For the third criterion the logistic company 'X' did not deliver the goods on time. So it did not fulfill the criterion according to the expected behavior. Hence the value of Eval<sub>Delivery</sub> is 0.

- For the fourth criterion the logistic company 'X' unpacked the goods at the destination address but did not arrange it at the destination address according to how the trusting peer 'A' wants. Hence the value of Eval<sub>Unpacking</sub> in this case is 0.

- For the fifth criterion the goods were delivered in the same condition as pickup. Hence the value of Eval<sub>Condition</sub> is this criterion will be 1.

- For the sixth criterion the logistic company provided with a track and trace facility to peer 'A'. Hence the value of the Eval<sub>Track</sub> is 1.

Now after determining the fulfillment of each criterion, peer 'A' will evaluate the familiarity of the logistic company 'X' with each criterion in its past interactions depending on the recommendations from other peers. Hence the value of  $Fam_{Criterion}$  for each criterion is as follows:

- According to the recommendation from peer 'C' the logistic company had packed its goods before. Hence the value of  $Fam_{Packing}$  is 2 according to table 2.
- According to recommendations from peer 'B' and 'C', the value of  $Fam_{Pickup}$  is 2.
- According to recommendation from Peer 'B' value of  $Fam_{Delivery}$  is 2.
- According to recommendation from Peer 'C' value of  $Fam_{Unpacking}$  is 2.
- According to recommendation from Peer 'C' value of  $Fam_{Condition}$  is 2.
- According to the recommendations from both Peer 'B' and Peer 'C' the value of  $Fam_{Track}$  is 1.

To find out the accuracy with which each criterion was communicated to the logistic company 'X' from peer 'A' the metric  $Accu_{Criterion}$  will be used. The value of  $Accu_{Criterion}$  for each criterion is as follows:

- Criterion 1 was communicated clearly. Hence the value of  $Accu_{Packing}$  is 1.
- Criterion 2 was communicated clearly. Hence the value of  $Accu_{Pickup}$  is 1.
- Criterion 3 was communicated clearly. Hence the value of  $Accu_{Delivery}$  is 1.
- Criterion 4 was NOT communicated clearly. Peer 'A' did not specify to the logistic company 'X' that it wants the goods to be arranged at the destination address. Hence the value of  $Accu_{Unpacking}$  is 0.
- Criterion 5 was communicated clearly. Hence the value of  $Accu_{Condition}$  is 1.
- Criterion 6 was communicated clearly. Hence the value of  $Accu_{Track}$  is 1.

Assigning the significance of each criterion according to the peer 'A', the values of  $Sig_{Criterion}$  are:

- A value of 1 to  $Sig_{Packing}$
- A value of 2 to  $Sig_{Pickup}$
- A value of 2 to  $Sig_{Delivery}$
- A value of 2 to  $Sig_{Unpacking}$
- A value of 2 to  $Sig_{Condition}$
- A value of 2 to  $Sig_{Track}$

In order to quantify numerically the actual behavior of the trusted peer in the interaction i.e. the assessment of commitment of fulfillment in the interaction ( $Asses_{Interaction}$ ) the individual assessment of the all the criterions should be added.

$$\begin{aligned} \text{Hence } Asses_{Interaction} = & \\ & (((Eval_{Packing} * Fam_{Packing}) * Accu_{Packing} * Sig_{Packing}) + \\ & ((Eval_{Pickup} * Fam_{Pickup}) * Accu_{Pickup} * Sig_{Pickup}) + \\ & ((Eval_{Delivery} * Fam_{Delivery}) * Accu_{Delivery} * Sig_{Delivery}) + \\ & ((Eval_{Unpacking} * Fam_{Unpacking}) * Accu_{Unpacking} * Sig_{Unpacking}) + \\ & ((Eval_{Condition} * Fam_{Condition}) * Accu_{Condition} * Sig_{Condition}) + \\ & ((Eval_{Track} * Fam_{Track}) * Accu_{Track} * Sig_{Track})) \end{aligned}$$

Substituting the respective values in the above equation:

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

$$Asses_{Interaction} = 12$$

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 was far from the promised commitment. For that it needs to find the best possible behavior ( $ProCom_{Interaction}$ ) which also shows the promised commitment that was expected in the interaction.

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

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

$$\begin{aligned} ProCom_{Interaction} = & \\ & (((ProCom_{Packing} * Fam_{Packing}) * Accu_{Packing} * Sig_{Packing}) + \\ & ((ProCom_{Pickup} * Fam_{Pickup}) * Accu_{Pickup} * Sig_{Pickup}) + \\ & ((ProCom_{Delivery} * Fam_{Delivery}) * Accu_{Delivery} * Sig_{Delivery}) + \\ & ((ProCom_{Unpacking} * Fam_{Unpacking}) * Accu_{Unpacking} * Sig_{Unpacking}) + \\ & ((ProCom_{Condition} * Fam_{Condition}) * Accu_{Condition} * Sig_{Condition}) + \\ & ((ProCom_{Track} * Fam_{Track}) * Accu_{Track} * Sig_{Track})) \end{aligned}$$

Substituting the respective values in the equation we get:

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

$$ProCom_{Interaction} = 16$$

Substituting the above values of  $Asses_{Interaction}$  and  $ProCom_{Interaction}$  in equation 2 to find out the Risk in the interaction due to the un-commitment in the trusted peer's actual behavior, we get:

$$Risk_{Interaction} = \frac{16-12}{16}$$

$$Risk_{Interaction} = \frac{4}{16}$$

$$Risk_{Interaction} = 0.25$$

Determining the percent of Risk in the interaction by using equation 3:

$$\text{Percent of Risk}_{Interaction} = (Risk_{Interaction} * 100)$$

$$\text{Percent of Risk}_{Interaction} = 25 \%$$

Mapping the Risk involved in the interaction to the Riskiness scale by using equation 4 to find out the Riskiness value of the trusted peer we get:

Riskiness Value = LEVEL (25%)

Riskiness Value = 4

Hence Riskiness value of the trusted peer 'X' according to the trusting peer 'A' is 4 on the Riskiness scale, which is assigned according to the level of its un-committed behavior in the interaction. This value also suggests that the trusted peer 'X' is *Largely UnRiskY*.

By the above example we see that:

- Criterion 4 was not communicated to the trusted peer by the trusting peer and subsequently that particular criterion was not taken into consideration while determining the promised commitment from the trusted peer by using the Accu<sub>Criterion</sub> metric, hence leaving it out when determining its Riskiness value.
- Criterion 3 was fulfilled by the trusted peer in its previous interaction, but was not fulfilled by it in this particular interaction. This shows that the Risk in dealing with this peer should be high. Hence that particular criterion is given more weight by the metric Fam<sub>Criterion</sub> while finding out the promised commitment, therefore assigning it a deserving Riskiness value at the end.

#### XIV. CONCLUSION

In this paper we first discussed about the need to analyze Risk in decentralized transactions. We then defined Risk and the term Riskiness in the context of Peer-to-Peer transactions. Further we defined a Riskiness scale and explained the individual levels of that scale and its corresponding semantics. We then proposed a methodology of Risk measurement in an interaction by using the defined metrics and we concluded by explaining the proposed methodology by using an example. By using the past or the current Riskiness value of the trusted peer, the trusting peer can predict the future Riskiness value of the trusted peer on the Riskiness scale before starting an interaction. That is our future work.

#### REFERENCES

- [1] I. Stoica, R. Morris, D.R. Karger, M.F. Kaashoek, H. Balakrishnan, "Chord: A Scalable Peer to Peer lookup service for internet applications" *Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp 149-160, San Diego, CA, USA, 2001.
- [2] A. Singh, L. Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems" *Proceedings of the Third IEEE International Conference on P2P Computing*, Linköping, pp. 142-149, Sweden, 2003.
- [3] F. Cornelli, E. Damiani, S.D.C. Vimercati, S. Paraboschi, P. Samarati, "Choosing Reputable Servants in a P2P Network", *Proceedings of the International WWW Conference (11), Honolulu, Hawaii, USA*, May 7-11 2002.
- [4] H. Chan, R. Lee, T.S. Dillon and E. Chang, "E-Commerce and its Applications", 1 edition, John Wiley and Sons, Ltd, 2002.
- [5] O.K. Hussain, E. Chang, B. Soh, and T.S. Dillon, "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.
- [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] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives", Making and Breaking Cooperative Relations, Basil Blackwell, New York, USA, 1988.
- [8] R.C. Mayer, J.H. Davis and F.D. Schoorman, "An interactive model for organizational trust", *Academy of Management Review*, vol. 20, no. 3, pp.709-734, 1995.
- [9] 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, pp. 391-404, 1998.
- [10] P. Sztompka, "Trust: A sociological theory", Cambridge University Press, Cambridge, U.K., 1999.
- [11] 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*, pp 193-204, New Orleans, USA, 2001.
- [12] C. Cheung and M.K.O. Lee, "Trust in Internet shopping: A proposed model and measurement instrument", *Proceedings of the 6th Americas Conference on Information Systems*, pp 681-689, August 10-13 2000.
- [13] K.J. Stewart, "Transference as a means of building trust in World Wide Web sites", *Proceedings of the International Conference on Information Systems*, Charlotte, USA, pp 459-464, 1999.
- [14] 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, pp 1-35, 1999.
- [15] S. Greenland, "Bounding analysis as an inadequately specified methodology", *Risk Analysis* vol. 24, no. 5, pp. 1085-1092, 2004.
- [16] R.M. Adler, "Distributed Coordination Models for Client/Server Computing", *Computer* 28, 4, pp. 14-22, 1995.
- [17] B. Leuf, "Peer to Peer, Collaboration & Sharing on the Internet", Pearson Education Pty Ltd, 2002.
- [18] 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>
- [19] M.E. Orlowska, "The Next Generation Messaging Technology – Makes Web Services Effective", *Proceedings of the Sixth Asia Pacific Web Conference*, pp. 13-19, Springer-Verlag Berlin Heidelberg 2004.
- [20] 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)*, 2004.
- [21] 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, June 2004.
- [22] 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 Service*, San Diego, USA, pp.26, 2004.
- [23] 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.
- [24] 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, Perth, 2005.
- [25] I. Ray and S. Chakraborty, "A Vector Model of Trust for Developing Trustworthy Systems", *Proceedings of the 9th European Symposium on Research in Computer Security*, pp 260-275, France, 2004.
- [26] 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.
- [27] 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*, pp 192-201, Hawaii, 2003.
- [28] M.P. Papazoglou, B.J. Kramer, and J. Yang, "Leveraging Web-Services and Peer-to-Peer Networks", *Proceedings of the Sixth Asia Pacific Web Conference*, Springer-Verlag, Berlin Heidelberg 2003.
- [29] D.F. Cooper, "The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:2004", Tutorial Notes: Broadleaf Capital International Pty Ltd. Available: [http://www.broadleaf.com.au/tutorials/Tut\\_Standard.pdf](http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf) 2004.
- [30] F.K. Hussain, E. Chang, and T.S. Dillon, "Classification of trust in peer-to-peer (P2P) communication", *International Journal of Computer Science Systems and Engineering*, Volume 19(1), pp. 59-72, March 2004.

- [31] O.K Hussain, E.Chang, F.K. Hussain, T.S. Dillon and B. Soh, "Context Based Riskiness Assessment", IEEE *TENCON 2005*, pp. 352-356, Melbourne, November 22-24 2005.
- [32] 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.