©2005 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

Risk in Trusted Decentralized 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, WA, Australia*
Email :{Omar.Hussain, Elizabeth.Chang, Farookh.Hussain}@cbs.curtin.edu.au
[2] *Faculty of Information Technology, University of Technology, Sydney, NSW, Australia*
Email: tharam@it.uts.edu.au
[3] *Dept of Computer Science and Computer Engineering, La Trobe University, VIC, Australia*
Email: ben@cs.latrobe.edu.au

Abstract

Risk is associated with almost every activity that is undertaken on a daily life. Risk is associated with Trust, Security and Privacy. Risk is associated with transactions, businesses, information systems, environments, networks, partnerships, etc. Generally speaking, risk signifies the likelihood of financial losses, human casualties, business destruction and environmental damages. Risk indicator gives an early warning to the party involved and helps avoid deserters. Until now, risk has been discussed extensively in the areas of investment, finance, health, environment, daily life activities and engineering. However, there is no systematic study of risk in Decentralised communication, which involves e-business, computer networks and service oriented environment. In this paper, we define risk associated with trusted communication in e-business and e-transactions; provide risk indicator calculations and basic application areas.

Keywords*:* Trust, Decentralized Peer-to-peer Communications, e-Business, Risk, Riskiness, Risk Indicator.

1. Introduction

In this paper, our main focus is on defining *Risk* in decentralized transactions in the area of Trusted Communication and e-Business, and define risk indicators and risk measurement, we also give preliminary advise on how and where to apply them. This paper is organized in nine sections. Section 2 reviews risk in information systems; Section 3 defines risk in a decentralized transaction and explains its constituting components in detail; Section 4 discusses the areas in which this definition of risk can be utilized; Section 5 briefly discusses the metrics by which the trusting peer can assign a Riskiness value to the trusted peer after the interaction; while Section 6 discusses the mathematical formulae of assigning Riskiness value by using those metrics, Section 7 speaks about the Risk analysis in e-commerce, Section 8 discusses about its impact and Section 9 concludes the paper.

2. Literature Review of Risk Study

In this section, we discuss the existing work on Risk study and we find all these methods have different interpretations of risk and, hence propose their own definitions for defining and measuring it. In this section, we restrict the definitions of risk which are closely related to the fields of computing, trusted communication, decentralised transactions, and e-Business. 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. Risk can be seen in two perspectives: the uncertainty of the outcome; and / or the cost of

Proceedings of the 21st International Conference on Data Engineering (ICDE '05)
1084-4627/05 $20.00 © 2005 IEEE

IEEE COMPUTER SOCIETY

the outcome, when it occurs, which is related to risk.

Risk has been defined in different ways by different researchers [2]. We will summarize some definitions of risk which are related to our discussion.

March and Shapira [3] define risk more by the magnitude of the value of the outcome rather than by taking its likelihood. This paradigm of risk is more common in business transactions.

Luhmann [4] defines risk in a transaction where the possible damage might be more than the advantage sought. This type of perception is more common in finance and investments where the expected returns are high.

Mayer, Davis and Schoorman [5] conclude that risk is present in the transaction only if the negative outcome outweighs the positive outcome at the end of the transaction.

In contrast to this definition, Rousseau, Sitkin, Burt and Camerer [6] measure risk as the potential negative consequence and probability of failure.

Sztompka [7] defines risk as the probability of the loss of the resources invested. This is a more general definition of risk which can be applied to every transaction in any field.

Grazioli and Wang [8] view risk as the consumers' perception of the uncertainty and adverse consequences of engaging in an activity.

Cheung and Lee [9] 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.

Stewart [10] classifies risk as channel risk and store risk. Channel risk is also referred as Internet and web risk. 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, Trctinsky and Vitale [11] define risk in IS by using items reflecting its likelihood such as too much uncertainty, how to characterize the decision to proceed with the transaction

Additionally, social dimensions of risk are addressed by social scientists [1].

There is still confusion in the relationship between Trust and Risk. As Mayer et al [5] suggest 'it is unclear whether risk is an antecedent to trust'. The inclusion of risk in the study of behaviour 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. Keeping this in view, we propose a definition of risk involved in a decentralized transaction in e-commerce.

3. Defining Risk in Trusted Decentralized Communications

Risk between two peers in P2P communication can be defined 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 transaction begins, resulting in the loss of $ and the resources involved in the transaction.

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

3.1 Trusting Peer

As described in Hussain, Chang and Dillon [12], *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 a transaction 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 transaction to begin. Hence, John is the *Trusting Peer* in this case.

3.2 Trusted Peer

As also described in Hussain et al [12], *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.

3.3 Not Act as Expected

When the trusting peer starts a transaction / or is going to start a transaction, he expects it to proceed and end in a certain way, based on the impression that he gets of the trusted peer during the course of reposing trust. This is termed *expected behaviour* [13], or when both the peers

IEEE COMPUTER SOCIETY

agree to behave in a certain way then it is known as *mutually agreed behaviour* [13]. This behaviour of the trusted peer motivates the decision of the trusting peer to a certain extent to proceed with the transaction or not.

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

3.4 Likelihood

Likelihood refers to possibility, or to some thing which is not clearly understood or too readily predicted. 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 a transaction 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 after the payment is received as she was supposed to, and then there is likelihood that she will not respond to him as expected and complete the transaction as expected.

3.5 Context

Context can be defined as the purpose for which the transaction is being held. When defining risk, it is important to take context into consideration, as risk can be dynamic and might not be the same for each context, as it varies according to the worth of the context of the transaction. When we are speaking of risk in a transaction between two peers, we take into consideration only that transaction, and not any other transaction between those two peers.

To illustrate this with an example, the above transaction between Mary and John is for an MP3 player. Hence, the *context* for the above transaction 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 in this transaction is the computer. Risk that was between John and Mary in the transaction of the MP3 player might not be the same in the transaction of the computer as this is a different context.

3.6 Particular Time

Time too is important when we are considering risk. Risk is dynamic and it is not possible for the trusting peer to have the same impression of the trusted peer throughout the transaction, which it had at a particular time. The impression or trust of the trusted peer by the trusting peer can either improve or degrade as the transaction progresses, scaling the risk associated with the transaction along with it.

For example, let us consider that before John starts the transaction of the MP3 player with Mary, he does not know her and, hence, the risk in the transaction might be high. So he takes recommendation from the other peers about Mary's capabilities and based on that he might get a better idea of the willingness and capability of the trusted peer, hence, scaling the risk accordingly with the impression achieved.

A second example can be taken of a scenario before the start of the MP3 player transaction between John and Mary. They might not know each other and, hence, the risk associated with the transaction might be very high. But on further interactions between them, the trusting peer might know the capability and willingness of the trusted peer to deliver on the expected behaviour, changing his opinion and the risk associated along with it. Suppose John and Mary meet again for a transaction with the context of a computer this time. After the completion of the transaction of the MP3 player, according to the mutually agreed behaviour, both the peers now know about each other's capability and the risk associated in this transaction might not be as high as compared to the previous interactions.

When we are speaking of risk at a particular time, we are capturing the dynamic nature of risk associated with the transaction at that particular instant.

4. Risk in Trusted e-Business and Communication

IEEE COMPUTER SOCIETY

Electronic transactions are usually done in a client server environment, where the server is the central host computer which performs all the tasks and clients are those machines which provide an interface to those servers and allow the user to proceed with the transaction. A transaction of this kind is called a *centralized transaction,* such as in eBay. In centralized transactions, the control is between the server and the client, whereas in a decentralized transaction the control is between the clients only, such as in Gnutella. These transactions resemble the early forms of the Internet in many ways and are regarded as the next generation of the Internet. Some of the characteristics of decentralized transactions are:

1. There is no server in this transaction between peers;
2. The peers interact with each other directly and the interactions are passed to them, rather than through a server as compared to a centralized transaction; and
3. The peers can forge or create multiple identities in a decentralized transaction and there is no way of checking how genuine the identity claimed by the peer. On the other hand, in a centralized transaction it can be checked as the information about the peers is stored in the server.

The above properties clearly show that a decentralized transaction carries more risks and, hence, merits more detailed investigation.

The definition of risk defined in the previous section is suited to areas in which the transactions are done in a decentralized or distributed environment, where no server is involved and the clients deal directly with each other. The clients can either deal with each other face-to-face or over the Internet without knowing each other. A few areas in which such decentralized transactions might be carried out include while establishing trust, peer-to-peer communication, e-business transactions, and transactions carried out on a secure network. In these areas this definition of risk applies effectively.

5. Risk Indicator

As explained 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. If there is a way by which they can know about the nature of the trusted peer then it will assist them greatly in making a decision to proceed with the transaction or not. By the 'nature of the trusted peer' we mean the risk that can be involved in dealing with this peer. In this paper, we try to alleviate this problem to a certain extent by proposing a method of assigning a *Riskiness* value to the trusted peer after the transaction, so that the trusting peer or any other peer might know before hand the level of risk that would be present in dealing with this peer. We define what the term *Riskiness* means and define seven different Riskiness levels. We also define the semantics associated with those levels and briefly propose the metrics by which a trusting peer can assign a Riskiness value to the trusted peer after the communication.

Riskiness of a peer is defined as *the numerical value that is assigned by the trusting peer to the trusted peer, which shows the level 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 in the Riskiness scale, which gives an indication to other peers about the nature of the peer and up to what level of risk is present in dealing with that peer.

In Table 1, we define seven 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.

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 ☆ to ★
Level 2	Partially Risky	$1 < x \leq 2$	From ★☆ to ★★
Level 3	Largely UnRisky	$2 < x \leq 3$	From ★★☆ to ★★★
Level 4	UnRisky	$3 < x \leq 4$	From ★★★☆ to ★★★★
Level 5	Very UnRisky	$4 < x \leq 5$	From ★★★★☆ to ★★★★★

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

IEEE COMPUTER SOCIETY

Our method of assigning Riskiness to a peer is through the notion of *expectations or promised commitment* (expected behaviour and mutually agreed behaviour respectively) and *actual commitment* (to what extent the trusted peer commits to the expected behaviour). In other terms, it can be said as expected behaviour versus actual behaviour. The greater the difference between these two behaviours the higher the level of risk present between them in the transaction and vice versa. In order to measure the degree of deviation, we will make use of the CCAS metrics.

Commitment of an Interaction (Com $_{Interaction}$)

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

Commitment of the Criterion (Com $_{Criterion}$)

The metric Com $_{Criterion}$ represents whether the trusted peer has fulfilled that specific criterion according to what was decided upon by using or promised to the trusting peer.

Accuracy of the Criterion Communication (Accu $_{Criterion}$)

Riskiness can be correctly analyzed when the trusted peer knows all the factors and bases against which he 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.

Significance of the Criterion (Sig $_{Criterion}$)

Another important factor to consider while finding out the deviation in an interaction is the Significance of the Criterion (Sig $_{Criterion}$). We define the metric Sig $_{Criterion}$ which expresses the significance of the criterion and gives the trusted peer an idea of factors which should be considered important. All the criterion of an interaction will not be of equal importance or significance. Some criterions 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 a transaction might depend on its capability of delivering on the outcome of the transaction.

6. Risk Measure

After finding out the value of the metric for each criterion, in order to properly quantify the Com $_{Interaction}$ against the Riskiness scale, we need to first find out how much the trusted peer's behaviour (which shows its committed behaviour for the interaction) deviates from the best possible committed behaviour that was expected from him (expected behaviour) or the promised commitment that the trusted peer agreed to (mutually agreed behaviour). We represent that behaviour as ProCom $_{Interaction}$ that was expected of him and which he could have shown or displayed. If we express the behaviour of the trusted peer relative to the best possible behaviour, then we get a measure that quantifies the behaviour of the trusted peer relative to the best possible behaviour. 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

$$\text{Risk}_{\text{Interaction}} = \frac{\text{Com}_{\text{Interaction}}}{\text{ProCom}_{\text{Interaction}}}$$

In order to map the behaviour of the trusted peer to the Riskiness scale, we need to map the Risk involved in the transaction to the Riskiness scale, which is of the range (-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 the interaction a value in the range of (0,5) should be assigned to the trusted peer by the trusting peer. Hence we have to map the Riskiness of the peer on the scale (0, 5). So in order to express the Riskiness value of a peer after the interaction on the scale (0, 5) we will

IEEE COMPUTER SOCIETY

multiply the Risk in the interaction $Risk_{Interaction}$ by 5. The value obtained can be a real number. In order to express it as a whole number we will round it off. Hence Riskiness value of the peer is expressed as:

$$\text{Riskiness Value} = \text{ROUND} \frac{(Com_{Interaction})}{(ProCom_{Interaction})} * 5$$

But as explained earlier the commitment in an interaction is a function of commitment of a criterion, the accuracy of criterion communication and significance of the criterion. Hence substituting those values in the equation we get:

Riskiness Value=

$$\text{ROUND} \sum_{I=1}^{n} \frac{(Com_{criterion\,I} * Accu_{Criterion\,I} * Sig_{Criterion\,I})}{(ProCom_{criterion\,I} * Accu_{Criterion\,I} * Sig_{criterion\,I})} * 5$$

7. Risk Analysis in e-Commerce

Risk is important in the study of behaviour 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 [1]. 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 sale of an item on the web is lower as the cost of the product gets higher. For higher cost items, the web does not tend to act as a medium to buy, but as a means for providing information to assist a purchasing decision and vice versa for lower cost items. The likelihood of a negative outcome might be the same in both the transactions, but the magnitude of the loss will be greater in the higher cost transaction. Thus, the relative reluctance of the customers to buy high cost items on the Internet as compared to the lower cost items would be consistent with the idea in practice, that the magnitude of potential loss appears to define the perception of risk and not the likelihood of loss [3].

8. Risk Analysis and Its Impact

Risk is defined in a number of different ways according to the context in which it is being discussed. Each transaction is associated with some kind of risk and, hence, it needs to be defined in accordance to that specific context, in order to analyze the correct amount of risk associated with it. 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 of exposure and other field data, computer modelling, and related social, economic and communication considerations.

Unfortunately, the methods for risk analysis in the area of evaluating health, environmental and engineering activities will not give us a meaningful answer when they are applied to determine the risk in the area of Computer Science.

9. Conclusion

In this paper, we discussed the term Risk in different contexts and in the field of Information Systems and summarized the term risk as defined by other researches in their work. We then defined risk in decentralized transactions for P2P communications and explained through use of an example. We also highlighted the area in which this definition might be applicable. We then defined the seven levels of Riskiness and gave a brief overview of the metrics which are utilized in finding the Riskiness value of the trusted peer.

10. References

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

[2] 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*

IEEE COMPUTER SOCIETY

International Conference on System Sciences, January 6-9 2003.

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

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

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] F.K. Hussain, E. Chang, and T.S. Dillon, 'Defining trust in peer-to-peer (P2P) communication', *Proceedings of the Fourth International Network Conference INC*, 2004, Plymouth, UK.

[13] 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.

IEEE COMPUTER SOCIETY