

© 2010 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A Fuzzy Approach for Transactional Risk Management in E-Business Collaborations

Omar Hussain

Digital Ecosystems and Business Intelligence Institute
Curtin University of Technology
Perth, Australia
e-mail: o.hussain@cbs.curtin.edu.au

Abstract— Risk Management is an important process to be carried out for any form of interaction before decision-making. This process will help the concerned user to take steps and actions accordingly in order to address risks and achieve the activity's desired goals. Various techniques and approaches for risk management have been discussed in the literature. But the process of risk management is not generic and it varies and changes according to the domain or purpose of the interaction for which it is being considered. E-business interactions are collaborative interactions that are mostly carried out over a virtual environment. But by considering the growth of e-business interactions, a process of risk management is needed by which the interacting user can actually minimize and lessen the level of risk before decision-making. In this paper, a quantitative approach for risk management in e-business interactions is proposed which the interacting user can utilize to lessen the level of risk and then make an interaction-based decision.

Keywords— *Perceived Risk, Performance Risk, Financial Risk, Risk Management.*

I. INTRODUCTION

The growth of e-business activities is quite evident by considering the statistics of its adoption and utilization by the users in the recent past [1, 2]. The primary reason for this is its capability of providing the users with enhanced functionality by which they can complete their tasks in much less time and with greater ease as compared to the previous interaction infrastructures. These functionalities continue to increase with the constant development and advancement of e-business interaction infrastructures, thereby increasing the advantages to the users. But apart from all the advantages that this interaction infrastructure provides, interacting users have to constantly look out for those factors that will produce a 'negative' outcome. A negative outcome signifies the interacting user's failure to achieve desired outcomes and the experience of losses. In order to minimize or alleviate the occurrence of such negative outcomes in e-business collaborative interactions, researchers have proposed the analysis of concepts such as trust [3, 4], security [5-7] and risk [8-10]. In this paper the focus of discussion is limited to the concept of risk.

Risk is a determinantal term that expresses the occurrence of those events that will result in the interacting user experiencing a negative outcome in its interaction. It will

also represent the level and magnitude of possible loss that an interacting user can experience as a result of it forming an interaction with a user. Once the level of risk in forming a business association risk has been analyzed, the interacting user will get an idea of the abovementioned two factors and then can utilize the analysis along with the determination of other concepts such as trust, security and privacy to make an informed interaction-based decision. But this step is possible only when the interacting user is comfortable or has the risk propensity to accept the level of risk that is determined in the business activity. If this is not the case, then the interacting user has to carry out the process of Risk Management. Risk management is the process by which the interacting user identifies the different levels of risk that are present in interacting with a user and then carries out steps by which it alleviates or minimizes them to a level which is then acceptable according to its risk propensity level. In the literature, various techniques have been proposed for risk management in different types of domains; but no approach has been proposed which the interacting user can utilize to effectively manage risk in the domain of e-business interactions. In this paper a quantitative approach for risk management in forming an e-business association is proposed. The proposed methodology is explained in the following sections. In Section 2, related work from the literature and the importance of risk management while decision-making is discussed. In Section 3, a brief overview of our previous work related with risk assessment is given. In Sections 4 to 6, a quantitative approach for risk management in e-business interactions is proposed. Finally, Section 7 concludes the paper.

II. RISK MANAGEMENT IN E-BUSINESS INTERACTIONS

In the process of risk analysis, risk management comes after the steps of risk identification, risk assessment and risk evaluation. As shown in Figure 1, Risk Management is an iterative process that takes the unacceptable level/s of risk in an interaction and then takes a series of steps to mitigate or alleviate them for a successful completion of a business activity. The un-acceptable level of risk in the interaction is dependent on the risk attitude, or risk propensity, or risk tolerance level of the interacting user. Risk attitude of the interacting user will show the level of risk which it is prepared to take, the level of consequences that it is ready to bear etc. Based on its risk attitude, the process of risk management is carried out on the identified level of risks.

Steps in Risk Analysis

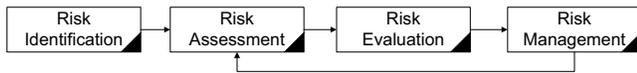


Figure 1. Steps in the process of Risk Analysis

While alleviating, minimizing or accepting risks the process of risk management is carried out against a set of goals to be achieved and the *expectations* of the interacting user as the result of the interaction. Approaches have been proposed in the literature for risk management in various domains such as project management, organizational risk etc. But those approaches are specific to the domain or problem in which they are being discussed. For example, risk management in the area of product development and management aims to first discuss the identified risks with the relevant stake holders and then develop strategies by which it can be avoided, deferred, diffused or shared [11]. Banks and Dunn discusses an approach for managing building risk where it provides suggestions by which the identified risks in security mechanisms are improved [12]. But such techniques are not suited to be applied for risk management in the domain of e-business interactions. The basic steps to take for risk management in the domain of e-business interactions might be the same as in other domains; but the process by which this is carried out is quite different. This is because, as the domain of the interactions change, the factors in which risk is analyzed changes, subsequently changing the process of risk management too. For example, the approaches for risk management in those domains mention that as soon as risk is identified, it should be discussed with the relevant stake holders, a dialogue should be established, risks should be prioritized and then steps should be developed for planning risk resolution. These steps for risk management are better suited for maintaining project risks or organizational risks where each actor involved has to do its part for the achievement of a common good. But this is not the case in an e-business interaction scenario. In an e-business interaction, it is the interacting initiating agent (or the risk assessing agent) that wants to achieve certain desired outcomes and therefore looks for an agent with which to form an interaction. In contrast to the other domains, there are no other agents involved that will be affected if it does not achieve what it wants, and subsequently the onus is on the risk assessing agent alone to ensure that it takes proactive steps once risk is identified to ensure that it will end up achieving what it wants at the end of its business activity.

In forming e-business associations, there are different types of risks in which the process of risk management has to be carried out. For example security risks, privacy risks etc. These types of risks represent the ‘operational risks’ present in forming the business activity and not the ‘transactional risks’ that are required for making an informed interaction-based decision. These two types of risks are different from each other and similarly the processes to manage them too vary. The focus of this paper is to manage transactional risk in forming a business association. But as discussed earlier, in

order to manage risks it is important to first determine it according to its object of analysis in the domain of interest. Approaches have been proposed in the literature which determine the level of transaction risk in e-business, but very few of them take into consideration both the subcategories of risk (probability of failure and consequences of failure) required for doing so. In other words, they determine the level of risk as a single subcategory outcome (either probability of failure or consequences of failure) [13-15] and do not take into consideration the context specific and dynamic nature of transactional risk. As a result, the risk that they determine does not represent the actual level/s of transactional risk in forming a business association. Subsequently any approach of risk management on those levels does not address all the risks required. In order to alleviate these drawbacks and have a comprehensive process of risk management in e-business interactions, in our previous work we have developed methodologies by which the interacting user in an e-business interaction can determine the different level/s of transactional risk by determining both its subcategories according to its context specific and dynamic characteristics. A brief overview of the work is presented in the next section.

III. TRANSACTIONAL RISK ANALYSIS IN FORMING E-BUSINESS ASSOCIATIONS

A user initiating an e-business interaction wants to achieve certain desired outcomes and, in order to achieve these, has to interact with another user who has the capability and who is willing to provide these outcomes to it. The interaction initiating user is termed the risk assessing agent and the user with whom it has to decide whether to interact with and hence analyses the level of risk as the risk assessed agent. There might a single risk assessed agent or a given set of risk assessed agents from which the risk assessing agent has to choose an agent with which to interact. The risk assessing agent can facilitate this decision-making process of choosing which agent to interact with by analyzing the level of transactional risk present in interacting with each of them. Transactional risk will represent the different levels of failure and the possible consequences of failure in interacting with a risk assessed agent. We proposed that the level of transactional risk in e-business interactions for decision making should be determined as a combination of two subcategories. They are a) Performance Risk, and b) Financial Risk.

Performance Risk: Performance risk represents the different levels of failure that the risk assessing agent can experience if it forms an interaction with a risk assessed agent. The performance risk is determined according to the expectations of the interaction, which represent the collection of all the desired outcomes of the risk assessing agent. Each desired outcome from the expectations is termed the ‘assessment criterion’. To determine the performance risk in forming an interaction with a risk assessed agent, the risk assessing agent takes into consideration each assessment criterion and then determines the level of failure of the risk assessed agent in committing to it as desired, in the different periods of time of its interaction [16]. Based on the

determined analysis, the *FailureLevel Curve* that represents the different levels of failure of the risk assessed agent in committing to each assessment criterion is determined.

Financial Risk: We consider that the risk assessed agent interacts with a risk assessing agent to give its desired outcomes in exchange of its financial resources which are negotiated while forming the expectations. Financial risk represents the different level/s of financial loss in those resources as a result of forming a business interaction with a risk assessed agent. The level of financial risk in the business activity depends on a) the performance risk of the risk assessed agent; and b) the deviation in the occurrence of non-dependable events. Performance risk represents the level of failure of risk assessed agent in committing to the assessment criteria of the expectations that are dependent on it for successful completion. These outcomes are known as the dependable events. But there might be other factors that are not dependent on the performance of the risk assessed agent, but will still contribute to the non-commitment of the expectations. We term these factors as the non-dependable events. To determine the financial risk, it is important for the risk assessing agent to take into consideration both these types of events. Further, the total financial risk should represent the variability of the different levels of financial losses that the risk assessing agent can experience over a given period of time, and not just represent the crisp financial loss that is represented by the Value at Risk (VaR) models. In our previous work, we developed comprehensive methodologies by which the risk assessing agent captures the variability of its investment over the interaction time period and captures the financial loss from both dependable [17] and non-dependable events [18].

Perceived Transactional Risk: Once the risk assessing agent determines the two sub-categories of perceived transactional risk, it should then combine them to ascertain the level of perceived transactional risk in its business activity. Perceived transactional risk represents the different levels and magnitudes of transactional risk present in forming the e-business association. For better and informed representation during the stage of risk management, we proposed that the risk assessing agent should have a numeric and semantic representation of perceived transactional risk. In Hussain et al. [19] we proposed an approach where the numeric level/s of perceived transactional risk is determined by possibility theory and semantic level/s of perceived transactional risk by using fuzzy set theory. The numeric level of perceived transactional risk is determined on a scale of 0-100 whereas the linguistic level of perceived transactional risk is determined across 6 fuzzy sets that are Extremely Low (EL), Low (L), Low Medium (LM), Medium High (MH), High (H) and Extremely High (EH). Once those levels are determined, the risk assessing agent can then utilize them to make an informed interaction-based decision in its business activity.

Making an Informed Risk-based Decision: Once the level/s of perceived transactional risk in forming a business association has been determined, the risk assessing agent should then evaluate it to determine whether or not they are acceptable to it. It is possible that in some cases the risk

assessing agent may be ready to accept the level of risk that is present in its business activity, whereas in other cases it might conclude that the level of determined risk is too high for its liking. In order to have such an analysis, the risk assessing agent should analyze the level of determined risk according to its risk appetite or risk attitude. The level of acceptable risk by the risk assessing agent varies according to its accurate risk propensity at that given point in time. In order to have such an analysis, we proposed in Hussain et al. [19] a fuzzy inference system that takes into consideration the risk propensity of the risk assessing agent and analyzes the determined levels of perceived transactional risk to give an output in the form of either *Proceed* or *Don't Proceed*. The output fuzzy set is followed by a strength value in the range of 0-100 % which shows the strength by which it fires according to the risk assessing agent's risk propensity. Based on the analysis, the risk assessing agent can make an informed decision about whether to interact with a risk assessed agent or to choose which agent to interact with from a given probable set.

But it is quite possible that the risk assessing agent may find itself in a scenario when deciding on an agent or while choosing an agent from a probable set, where the given output from the fuzzy inference system is not a crisp *100% Proceed*. There might be some tendency towards the fuzzy set *'Don't Proceed'*. In other words, this implies that there are some levels of risk present in its e-business interaction with the risk assessed agent in question; that are beyond its risk appetite or risk propensity. A question arises of what the risk assessing agent should do in such scenarios. It cannot just randomly choose an agent with which to form an interaction as the level of risk present is more than what it can bear. Rather, it should carry out a series of steps known as Risk Management to reduce the determined levels of risks for making an informed interaction-based decision.

IV. MANAGING PERCEIVED TRANSACTIONAL RISK IN E-BUSINESS INTERACTIONS

As represented in Figure 2, the determined level/s of perceived transactional risk in the business activity are due to the financial risk in the business activity; which in turn is dependent on the performance risk of the risk assessed agent in dependable events and the deviation in the occurrence of non-dependable events. To have an effective process of risk management, the risk assessing agent should start it from that point where risks are initialized. In an e-business interaction, these can originate from a) Non-commitment of the dependable events and b) Deviation in the occurrence of non-dependable events.

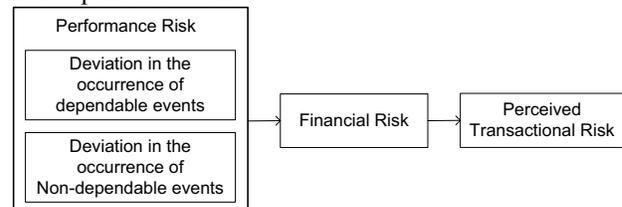


Figure 2. Process of determining perceived transactional risk in e-business interactions

In this paper, the discussion is limited to proposing an approach for risk management due to the non-commitment of the dependable events.

For carrying out the process of risk management, the risk assessing agent has to analyze each assessment criterion individually from its expectations and then analyze and determine if it has the capability of constituting a risk in its interaction. In order to achieve that, the following iterative process should be carried out:

A. Identify each dependable assessment criterion from its expectations.

This step will identify all the assessment criteria from the expectations that are dependent on the risk assessed agent for achieving a successful completion.

B. Determine the performance risk of the risk assessed agent in committing to the assessment criteria as promised, in each time slot of its interaction.

In this step, the risk assessing agent should determine the level of failure that it can experience in achieving a dependable assessment criterion if it forms an interaction with the risk assessed agent. 'Level of failure' represents the degree and magnitude of the risk assessed agent's inability to commit to the assessment criteria as decided upon when forming the expectations. This process is repeated for all the identified dependable assessment criteria. Further, the risk assessing agent should determine the incapability of the risk assessed agent in each time slot of the time space of its interaction with the risk assessed agent, to consider its dynamic nature. By doing so, it takes into consideration the variability in the incapability of the risk assessed agent to commit to an assessment criterion over the total time period of its business interaction.

C. Determine the significance of the assessment criteria.

The assessment criteria play an important and significant role during the process of risk management. From the perspective of the risk assessing agent, all the assessment criteria in its expectations may not necessarily be of equal importance. It may be the case that some assessment criteria from its expectations are more important than the others and the risk assessing agent may regard that if they are not fulfilled, then that may result in a high level of perceived transactional risk when interacting with the risk assessed agent. On the other hand, it could be the case that there are some assessment criteria which have a minimal impact on determining the outcome of the interaction. Further, it is possible that an assessment criterion that is considered being important by the risk assessing agent in a time slot may not be as significant in the next time slot. The importance of each assessment criterion in an interaction may vary because of the influence that it has on the outcome of the interaction at that given point in time [20]. Similarly, the process and severity of risk management for an assessment criterion at a given point of time too will vary according to its significance at that point in time.

D. Determine its Risk Attitude at different periods of time of its interaction.

This is the most important input while carrying out the process of risk management. Risk attitude of the risk assessing agent shows its inclination towards taking risks in the business activity. It is possible that the risk assessing agent might not be able to completely remove risks from its interaction. But it is possible that it might reduce or minimize the level of risks to a certain level that is 'acceptable' to it. If it reaches that point, then it can stop the process of risk management and choose that agent with which to form an interaction. So while undertaking risk management, the risk attitude of the risk assessing agent defines its current risk-taking tendency towards taking the level of risks in an interaction. It also represents how the risk assessing agent 'sees' the level of perceived transactional risk determined in forming an interaction with the risk assessed agent, and based on that, which levels of perceived transactional risk are acceptable to it and which are not. It is important to note that no two risk assessing agents might have the same risk attitude, and with the variation in their risk attitudes, their approach to risk management in the interaction varies. Further, the risk attitude of a risk assessing agent might not be the same throughout its interaction. It might vary according to the different scenarios, different assessment criteria or different time periods of its interaction with the risk assessed agent, also changing the process of risk management accordingly.

As the e-business association between the agents might extend to a point of time in the future, the risk assessing agent should carry out the process of risk management for each time slot of its interaction, and not for the overall total time period of the interaction as a whole. By doing so, the risk assessing can identify clearly the exact period of time in its interaction where the occurrence of a particular assessment criterion is beyond its acceptable limits, which in turn results in the occurrence of risk in the overall business interaction, and treat it accordingly. If the FailureLevel of the assessment criterion is beyond its acceptable limits, then the risk assessing agent has to develop recommendations or alternative steps and carry out the process of risk management so that the level of risk is brought back within its acceptable limits. By having such a repetitive process of risk management, the risk assessing agent will take into account the variability in the occurrence of each assessment criterion in the different time periods of its interaction, and take into consideration scenarios where the performance risk of an assessment criterion might be acceptable in one time slot but not in the other. Based on the analysis, it can take risk management action accordingly.

Once the risk assessing agent identifies all the above mentioned input factors, then it needs to determine whether the FailureLevel of an assessment criterion is beyond its acceptable limits. For that a method is needed that maps the input factors to the output space. A fuzzy inference system has been chosen to assist the risk assessing agent in determining that and with the process of risk management of

the dependable events of an e-business interaction. The proposed methodology is explained in the next section.

V. A FUZZY INFERENCE SYSTEM FOR RISK MANAGEMENT IN E-BUSINESS INTERACTIONS

The fuzzy system to determine whether the FailureLevel of an assessment criterion is within the acceptable limits takes in 3 inputs and gives a single output as shown in Figure 3. Each of the input factors influences the output value of acceptability that is generated.

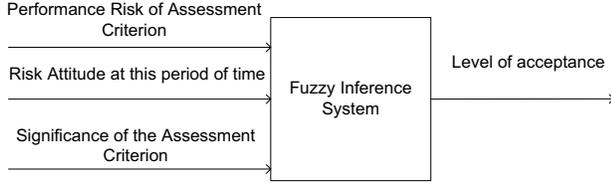


Figure 3. Overview of the Fuzzy Inference System for Risk Management

There are two broad categories of fuzzy-reasoning systems that need to be considered for the particular problem, and these are:

- 1) Mamdani method;
- 2) Takagi and Sugeno method.

In both approaches, the input conditions are given in the form of fuzzy sets partitioned on the input UoD. In the Mamdani approach, the output is in the form of a fuzzy-set partition on the output UoD, whereas in the case of the Takagi–Sugeno inference model, the output is a linear crisp function. In the current problem, an output that is represented by a single value that shows whether or not the level of performance risk in a dependable assessment criterion in a given time slot is acceptable to the risk assessing agent according to its risk propensity is desired. Furthermore, if it is not, then by what margin; so that the process of risk management is done accordingly. Hence, Takagi–Sugeno approach that produces a single crisp value which shows the level of acceptability is a more practical approach in that it would be more helpful and understandable by the risk assessing agent. Further, another reason for choosing Takagi Sugeno approach is that in Mamdani approach there are several different approaches by which the process of aggregation and defuzzification can be carried out, each of which might give somewhat different values for the output. So to avoid that, the first order Takagi and Sugeno approach was chosen. The Takagi–Sugeno (T–S) form of the rule is:

$$\text{If } (x_1 \text{ is } X_1 \text{ and } \dots, x_n \text{ is } X_n) \text{ then } (y_q = a_{q0} + a_{q1x_1} + \dots + a_{qn x_n})$$

where:

x_1, x_2 are scalar inputs;

X_1, X_2 are fuzzy sets;

$a_{q0}, a_{q1}, \dots, a_{qn}$, are real numbers; and

y_q is the consequent of the rule.

This is the form of the fuzzy-logic rule that was initially proposed by Takagi–Sugeno in their original work [21]. In the singleton case, the output y_q takes the form $y_q = a_{q0}$. A

fuzzy inference system with m fuzzy rules of the T–S form is considered. The form of the crisp output is:

$$Y(x) = \frac{\sum_{q=1}^m \alpha_q (a_{q0} + \sum_{s=1}^n a_{qsx_s})}{\sum_{q=1}^m \alpha_q}$$

α_q is the firing strength of rule q . The actual approach to fuzzy reasoning, in this case, has the following steps:

- 1) fuzzify inputs;
- 2) obtain the firing strength α_q associated with each rule q ;
- 3) obtain the output function of y_q associated with each rule q using the firing strength α_q ;
- 4) obtain the overall output $y(x)$.

To develop the fuzzy inference system, adaptive-network-based fuzzy-inference system (ANFIS) that is implemented in the fuzzy logic toolbox of MATLAB is used. One characteristic of the ANFIS is that it generates the membership function of each variable of the underlying fuzzy inference system according to the set of data that is given to train it. The risk assessing agent can utilize this characteristic and take into consideration the context- and time-specific properties associated with risk and its interaction, when developing a fuzzy inference system to manage it. This is another advantage of using the Takagi Sugeno approach over the Mamdani approach for risk management, where the risk assessing agent can train the fuzzy set according to the specific characteristics of its interaction, to carry out the process of risk management.

In order to train the FIS, the risk assessing agent utilizes the past experiences that it has while interacting within the specific context of the interaction. These data points represent the input values of each input and, based on that, the subsequent level of acceptance by the risk assessing agent according to its risk propensity. Alternatively, the risk assessing agent can generate a set of data points according to its specific interaction with the risk assessed agent and then utilize them to train the FIS. Once the FIS is trained, then the membership functions of the input variables should be plotted. For the current problem, the risk assessing agent considers:

1. Trapezoidal shape membership function for Performance risk of the risk assessed agent in each assessment criterion, on the range of 0-100. The membership function should be divided into 6 fuzzy sets, namely Extremely Low, Low, Low Medium, Medium High, High and Extremely High as shown in Figure 4.

2. Combination of triangle and straight lines to represent the membership function for the Risk attitude of the risk assessed agent in each assessment criterion. The range of the membership function should be 0-5 and be divided into 3 fuzzy sets namely, Risk Averse, Risk Neutral and Risk Taking as shown in Figure 5. Each value within the range of 0-5 will represent a different level of risk attitude of the risk assessing agent subsequently implying that it accepts a different level of performance risk. In Table 1, the levels of perceived transactional risk which the risk assessing agent

will accept based on the different levels of its risk attitude are defined. These levels will be utilized by the fuzzy inference system while assessing a given assessment criterion at a given point in time according to the risk assessing agent's attitude.

3. Trapezoidal shape memberships function for the significance of each assessment criterion, within the range of 0-10. The membership function should be divided into 5 fuzzy sets, namely Minor Significance, Moderately Significant, Largely Significant, Major Significance and Extremely Significant as shown in Figure 6.

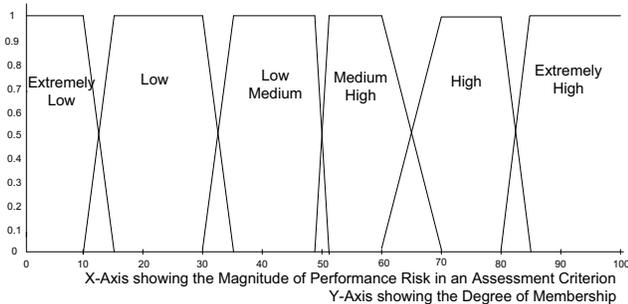


Figure 4. Membership Function for Performance Risk in an assessment Criterion

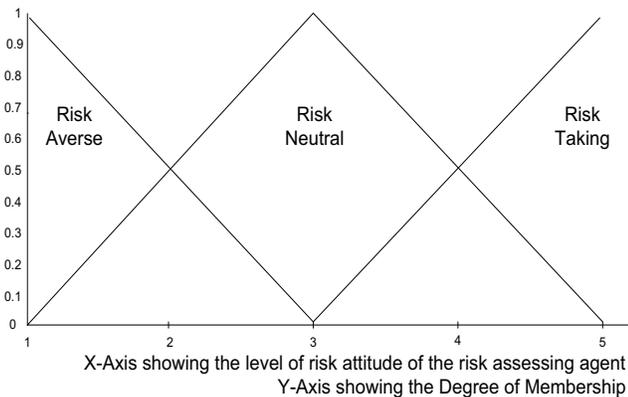


Figure 5. Membership Function for Risk Attitude of the Risk Assessing Agent

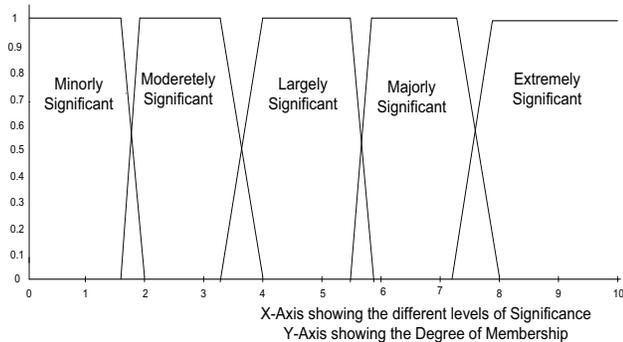


Figure 6. Membership Function for Significance of an Assessment Criterion

	Risk Attitude		Acceptable Level of Performance Risk
If	RA=1	then	EL=1
If	RN=0.1	then	L=0.2
If	RN=0.2	then	L=0.4
If	RN=0.3	then	L=0.6
If	RN=0.4	then	L=0.8
If	RN=0.5	then	L=1
If	RN=0.6	then	LM=0.2
If	RN=0.7	then	LM=0.4
If	RN=0.8	then	LM=0.6
If	RN=0.9	then	LM=0.8
If	RN=1	then	LM=1
If	RT=0.1	then	MH=0.34
If	RT=0.2	then	MH=0.67
If	RT=0.3	then	MH=1
If	RT=0.4	then	H=0.34
If	RT=0.5	then	H=0.67
If	RT=0.6	then	H=1
If	RT=0.7	then	EH=0.34
If	RT=0.8	then	EH=0.67
If	RT=0.9	then	EH=0.99
If	RT=1	then	EH=1

Table 1 showing the level of acceptance of performance risk according to risk attitude

The output of the FIS, 'Level of acceptance by the risk assessing agent' is represented by a single value within the range of 0-1. 0 means that the performance risk of the risk assessed agent in the assessment criterion is acceptable to the risk assessing agent according to its risk taking attitude, whereas 1 represents otherwise; and that the risk assessing agent has to carry out the steps of risk management for that assessment criterion and at that point in time. The higher the value of the output variable greater than 0 represents, the higher the level of unacceptable risk is present according to its risk attitude. Once this step is complete, the risk assessing agent should then test the developed FIS with another set of data to average the testing error. If the error is within the acceptable threshold, then the risk assessing agent can utilize the developed FIS to carry out the process of risk management, according to the specific characteristics of its e-business interaction.

In the next section, the working of the fuzzy inference system for risk management is explained with a business interaction.

VI. FUZZY INFERENCE SYSTEM FOR RISK MANAGEMENT

In order to explain the simulation of the FIS for risk management, let us consider the following e-business interaction scenario. Risk assessing agent 'A' wants to interact with a logistics company 'B' in order to move its goods from London, England to Perth, Australia from 1/2/2009 till 5/2/2009. Before doing so, agent 'A' wants to analyze the level of risk when deciding upon the logistics company with which it will form an interaction. Let us consider the expectations which agent 'A' forms after negotiations with the risk assessed agents are:

- The logistics company should pack the goods properly at the pick up address (C1).

- The goods should reach the destination in 5 days (C2).
- The logistics company should provide a track and trace facility (C3).
- The total cost for transferring the goods is 6000 Euros. Agent ‘A’ should pay half of the amount when the goods are picked up. Once the goods are delivered, Agent ‘A’ should make the remaining payment of 3000 Euros in equivalent Australian Dollars to the logistics company’s branch office in Perth on 5/2/2009 (C4).

The time space of the interaction is 5 days. To consider the dynamic nature of risk when performing risk analysis and risk management, the risk assessing agent divides the time space into 5 time slots, each of one day as shown in Figure 7.

| Time slot |
|-----------|-----------|-----------|-----------|-----------|
| T1 | T2 | T3 | T4 | T5 |
| 1/2/2009 | 2/2/2009 | 3/2/2009 | 4/2/2009 | 5/2/2009 |

Figure 7. Showing the time space of the interaction

From the expectations, assessment criteria (C1-C3) are dependable criteria on the risk assessed agent for their successful completion. Assessment criterion C4 comes under the non-dependable assessment criteria of the interaction. For risk analysis, the risk assessing agent considers the methodologies mentioned in Section III to determine the transactional risk and map it according to its risk attitude. Let us consider that the output that it obtains from the decision-making methodology is Proceed (73.70%) and Don’t Proceed (26.30%). So it has to carry out the process of risk management in order to ensure that whatever the level of risk is present in interacting with logistics company ‘B’ is within its acceptable limits. Due to space limitations, in this paper the working of the FIS for risk management for only assessment criterion C3 is shown.

As mentioned earlier, when carrying out the process of risk management, the risk assessing agent should take each dependable assessment criterion and then determine the performance risk of the risk assessed agent, its significance and its risk attitude in each time slot of its business activity. Let us consider that for assessment criterion C3, the risk assessing agent finds:

For time slot T1:

Performance risk (PR) of the risk assessed agent: 40% (on a scale of 0-100)

Significance (S) of the assessment criterion: 10 (on a scale of 0-10)

Risk attitude (RA) of the risk assessing agent: 1.1 (on a scale of 0-5)

For time slot T2:

PR of the risk assessed agent: 50% (on a scale of 0-100)

S of the assessment criterion: 10 (on a scale of 0-10)

RA of the risk assessing agent: 1.0 (on a scale of 0-5)

For time slot T3:

PR of the risk assessed agent: 55% (on a scale of 0-100)

S of the assessment criterion: 10 (on a scale of 0-10)

RA of the risk assessing agent: 0.9 (on a scale of 0-5)

For time slot T4:

PR of the risk assessed agent: 55% (on a scale of 0-100)

S of the assessment criterion: 10 (on a scale of 0-10)

RA of the risk assessing agent: 0.9 (on a scale of 0-5)

For time slot T5:

PR of the risk assessed agent: 50% (on a scale of 0-100)

S of the assessment criterion: 10 (on a scale of 0-10)

RA of the risk assessing agent: 0.8 (on a scale of 0-5)

Based on the above values of the inputs, the output of the FIS for assessment criterion C3 in each time slot are as given in Table 2.

Time slot	Input to the FIS (PR,S, RA)	Output of the FIS
T1	(40,10,1.1)	0.3
T2	(50,10,1)	0.46
T3	(55,10,0.9)	0.58
T5	(55,10,0.9)	0.58
T5	(50,10,0.8)	0.63

Table 2: showing the output of the FIS for risk management

From the above analysis it can be seen that the risk in the occurrence of assessment criterion C3 is beyond the risk attitude of agent ‘A’ in each time slot of its interaction. The level of variance from its risk attitude is represented by the deviation of the output from 0. Agent ‘A’ has to take steps by which the risk in each time slot in assessment criterion C3 is minimized that will in turn minimize the overall perceived transactional risk in its business activity. The steps to be taken are specific to the way by which the risk assessing agent wants to reduce the level of risk. It is possible to develop a standardized process for risk minimization as each interaction is different according to the purpose for which it is carried or interacting agent who is carrying it out. It should be noted that the above output from the FIS is according to the specific input values for the input variables given, and it changes with any change in the input values. For example assessment criterion C1 might be significant to the risk assessing agent only in the first time slot of its interaction and not so much in the other time slots. In such cases, its risk attitude towards it changes accordingly, scaling the process of risk management accordingly. The risk assessing agent should carry out such process on the other assessment criterion C1 and C2 and then carry out any recommendations on it accordingly to minimize or alleviate the level/s of risks. Doing so helps the risk assessing agent to identify and manage and address the risks according to each assessment criterion, thus helping it to carry out an effective process of risk management. This is different from the approaches proposed in the literature which aim to manage risk in the overall interaction at one go rather than considering each assessment criterion and doing it iteratively in each time slot of the interaction.

VII. CONCLUSION

Risk management is an important step to consider when making decisions regarding any form of interaction. Carrying out such a process will help the interacting user to successfully identify the negative factors present in its business interaction and then develop strategies by which these can be addressed or minimized so that the overall level of risk is within its risk attitude. In this paper, an approach for carrying out an effective process of risk management in e-business interactions was proposed. The proposed approach is limited to the dependable assessment criteria and utilizes a FIS, the performance risk, significance of the assessment criterion and the risk attitude of the risk assessing agent to determine the level of acceptability to it. The risk assessing agent can utilize the determined analysis to develop strategies by which it can address the levels of risk. The proposed approach in this paper is limited to the dependable events of an e-business interaction. In order to have a comprehensive approach for risk management, the developed methodology should also consider the non-dependable events. This is the future work.

REFERENCES

- [1] Australian Bureau of Statistics, "Online Shopping Blooms," in *Use of the Internet by Householders*, Australia, Nov 2000.
- [2] Reineke Reitsma, "European Online Shopping Landscape 2007," in *Forrester Research*, 2007.
- [3] Karl Aberer and Z. Despotovic, "Managing trust in a Peer-2-Peer Information System," Atlanta, Georgia, USA, 2001, pp. 310 - 317.
- [4] Anwitaman Datta, Manfred Hauswirth, and Karl Aberer, "Beyond 'web of trust': Enabling P2P E-commerce," Newport Beach, CA, USA, 2003, pp. 303-312.
- [5] Yudistira Asnar, Paolo Giorgini, and A. Mulyanto, "Risk in Secure and Dependable System: a Survey," Bandung, Indonesia, 2007.
- [6] Christian Schläger, Manuel Sojer, Björn Muschall, and G. Pernul, "Attribute-based Authentication and Authorisation Infrastructures for E-Commerce Providers," Krakow, Poland, 2006, pp. 132-141.
- [7] Nathan Dimmock, András Belokosztolszki, David Eyers, Jean Bacon, and K. Moody, "Using trust and risk in role-based access control policies," in *Ninth ACM symposium on Access control models and technologies* New York, 2004, pp. 156-162.
- [8] Li Xiong and L. Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities," in *International Conference on E-Commerce Technology (CEC'03)*, IEEE, Ed. Newport Beach, California, USA 2003, pp. 275-284.
- [9] Iain Gourlay, Karim Djemame, and J. Padgett, "Reliability and Risk in Grid Resource Brokering," Phitsanulok, Thailand, 2008, pp. 437-443.
- [10] Iris Bohnet and Richard Zeckhauser, "Trust, risk and betrayal," *Journal of Economic Behavior & Organization*, vol. 55, pp. 467-484, 2004.
- [11] Preston G. Smith and Guy M. Merritt, *Proactive Risk Management, Controlling Uncertainty in Product Development*: Productivity Press, 2002.
- [12] Erik Banks and Richard Dunn, *Practical Risk Management*: John Wiley, 2003.
- [13] Jeff C. Fan, "Trust and Electronic Commerce - A Test of an E-Bookstore," in *International Conference on e-Business Engineering (ICEBE'06)*, IEEE, Ed. Hong Kong: IEEE, 2006, pp. 110-117.
- [14] Brian J. Corbitt, Theerasak Thanasankit, and Han Yi, "Trust and e-commerce: a study of consumer perceptions," *Electronic Commerce Research and Applications*, vol. 2, pp. 203-215, 2003.
- [15] Cristiano Castelfranchi and R. Falcone, "Trust Is Much More than Subjective Probability: Mental Components and Sources of Trust," Hawaii, 2000, pp. 1-10.
- [16] Omar Khadeer Hussain, Elizabeth Chang, Farookh Khadeer Hussain, and Tharam S. Dillon, "A methodology to quantify failure for risk-based decision support system in digital business ecosystems," *Data & Knowledge Engineering*, vol. 63, pp. 597-621, December 2007.
- [17] Omar K. Hussain, Elizabeth Chang, Farookh K. Hussain, and Tharam S. Dillon, "Towards Quantifying the Possible Risk in e-commerce Interactions for RDSS," in *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'07)*, IEEE, Ed. Hong Kong, China: IEEE, 2007, pp. 89-96.
- [18] Omar Hussain and Tharam Dillon, "Ascertaining the Financial Loss from Non-dependable Events in Business Interactions by using the Monte Carlo method," Fukuoka, Japan 2009, pp. 406-411.
- [19] Omar Khadeer Hussain, Tharam S. Dillon, Farookh Khadeer Hussain, and Elizabeth Chang, "Transactional Risk-based Decision Making System in E-Business Computing," *Computer Systems Science and Engineering*, vol. 25, pp. 15-25, 2010.
- [20] Elizabeth Chang, Tharam Dillon, and F. K. Hussain, *Trust and Reputation for Service-Oriented Environments*. West Sussex, England: John Wiley & Sons, Ltd, 2006.
- [21] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modelling and control," *IEEE Trans. Syst., Man, Cybernetics*, vol. 15, pp. 116-131, 1985.