

Communicating Recommendations in a Service-Oriented Environment

Omar Khadeer Hussain

Curtin University of Technology, Australia

Elizabeth Chang

Curtin University of Technology, Australia

Farookh Khadeer Hussain

Curtin University of Technology, Australia

Tharam S. Dillon

University of Technology, Sydney, Australia

INTRODUCTION

The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:2004 (Cooper, 2004), 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 risks resulting from past, current, anticipated, or future activities. The use of these evaluations includes providing information for determining regulatory actions to limit risk, and for educating the public concerning particular risk issues. Risk analysis is an interdisciplinary science that relies on laboratory studies, collection, and exposure of data and computer modeling.

Chan, Lee, Dillon, and Chang (2002) state that 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 architectures through which e-commerce transactions can be conducted. They are: (a) client-server business architecture, and (b) peer-to-peer business architecture.

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 also applies to the transactions in the field of e-commerce and peer-to-peer business. In this article we will emphasize transactions carried out in the peer-to-peer business architecture style, as our aim is to analyze risk in such transactions carried out in a service-oriented environment.

Peer-to-peer (P2P) architecture is so called because each node has equivalent responsibilities (Leuf, 2002). This is a type of network in which each workstation or peer has equivalent capabilities and responsibilities. This differs from client/server architecture, in which some computers or

central servers are dedicated to serving others. As mentioned by Oram (2001), 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 type of transaction between peers.
2. Peers interact with each other directly, rather than through a server, as compared to a centralized transaction where the authenticity can be checked.
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 investigation. Similarly, in a service-oriented peer-to-peer financial transaction, there is the possibility of the trusted agent engaging in an untrustworthy manner and in other negative behavior at the buyer's expense, which would result in the loss of the buyer's resources. This possibility of failure and the degree of possible loss in the buyer's resource is termed as risk. Hence, risk analysis is an important factor in deciding whether to proceed in an interaction or not, as it helps to determine the likelihood of loss in the resources involved in the transaction.

Risk analysis by the trusting agent before initiating an interaction with a trusted agent can be done by:

- determining the possibility of failure of the interaction, and
- determining the possible consequences of failure of the interaction.

Figure 1. The riskiness scale and its associated levels

Riskiness Levels	Magnitude of Risk	Riskiness Value	Star Rating
Unknown Risk	-	-1	Not Displayed
Totally Risky	91-100% of Risk	0	Not Displayed
Extremely Risky	71-90% of Risk	1	From  to 
Largely Risky	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 

The trusting agent can determine the possibility of failure in interacting with a probable trusted agent either by:

- considering its previous interaction history with the trusted agent, if any, in the context of its future interaction, or
- soliciting recommendations for the trusted agent in the particular context of its future interaction, if it does not have any previous interaction history with it.

When the trusting agent solicits for recommendations about a trusted agent for a particular context, then it should consider replies from agents who have previous interaction history with the trusted agent in that particular context. The agents replying back with the recommendations are called the *recommending agents*. But it is possible that each recommending agent might give its recommendation in its own way, and as a result of that, it will be difficult for the trusting agent to interpret and understand what each element of the recommendations mean. Hence, a standard format for communicating recommendations is needed so that it is easier for the trusting agent to understand and assimilate them. Further, the trusting agent has to determine whether the recommendation communicated by the recommending agent is trustworthy or not before considering it.

In this article we propose a methodology by which the trusting agent classifies the recommendation according to its trustworthiness. We also define a standard format for communicating recommendations, so that it is easier for the trusting agent to interpret and understand them.

BACKGROUND

Security is the process of providing sheltered communication between two communicating agents (Singh & Liu, 2003;

Chan et al., 2002). We define *risk* in a peer-to-peer service-oriented environment transaction as the likelihood that the transaction might not proceed as expected by the trusting agent in a given context and at a particular time once it begins resulting in the loss of money and the resources involved in it. The study of risk cannot be compared with the study of security, because securing a transaction does not mean that there will be no risk in personal damages and financial losses. Risk is a combination of:

- the uncertainty of the outcome; and
- the cost of the outcome when it occurs, usually the loss incurred.

Analyzing risk is important in e-commerce transactions, because there is a whole body of literature based on rational economics that argues that the decision to buy is based on the risk-adjusted cost-benefit analysis (Greenland, 2004). Thus it commands a central role in any discussion of e-commerce that is related to a transaction. Risk plays a central role in deciding whether to proceed with a transaction or not. It can broadly be classified as an attribute of decision making that reflects the variance of its possible outcomes.

Peer-to-peer architecture-type transactions are being described as the next generation of the Internet (Orlowska, 2004). Architectures have been proposed by researchers (Qu & Nejdl, 2004; Schmidt & Parashar, 2004; Schuler, Weber, Schuldt, & Schek, 2004) for integrating Web services with peer-to-peer communicating agents like Gnutella. However, as discussed earlier, peer-to-peer-type transactions suffer from some disadvantages, and risk associated in the transactions is one of them. Hence, this disadvantage has to be overcome so that they can be used effectively with whatever service they are being integrated with.

Through the above discussion, it is evident that risk analysis is necessary when a transaction is being conducted in a

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/communicating-recommendations-service-oriented-environment/17061

Related Content

Biometric Authentication Methods on Mobile Platforms: An Introduction to Fingerprint Strong Feature Extraction

Agnitè Maxim Wilfrid Straiker Edoh, Tahirou Djara, Abdou-Aziz Sobabe Ali Tahirouand Antoine Vianou (2023). *International Journal of Mobile Computing and Multimedia Communications* (pp. 1-16). www.irma-international.org/article/biometric-authentication-methods-on-mobile-platforms/334130

Advances of the Location Based Context-Aware Mobile Services in the Transport Sector

Georgios Patris, Vassilios Vescoukisant Maria Giaoutzi (2011). *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (pp. 170-185). www.irma-international.org/chapter/advances-location-based-context-aware/48350

Mobile Big Data: A New Frontier of Innovation

Shivom Aggarwaland Abhishek Nayak (2016). *Emerging Perspectives on the Mobile Content Evolution* (pp. 138-158). www.irma-international.org/chapter/mobile-big-data/137993

Neighborhood-Based Route Discovery Protocols for Mobile Ad Hoc Networks

Sanaa A. Alwidian, Ismail M. Ababnehand Muneer O. Bani Yassein (2013). *International Journal of Mobile Computing and Multimedia Communications* (pp. 68-87). www.irma-international.org/article/neighborhood-based-route-discovery-protocols/80428

Mobile Learning in Health Professions Education: A Systematic Review

Zarrin Seema Siddiquiand Diana Renee D. Jonas-Dwyer (2013). *Pedagogical Applications and Social Effects of Mobile Technology Integration* (pp. 193-205). www.irma-international.org/chapter/mobile-learning-health-professions-education/74912