Trust and Reputation Relationships in Service-Oriented Environments

Elizabeth Chang[1], MIEEE, Tharam S Dillon[2], FIEEE and Farookh Khadeer Hussain[3]
[1] *School of Information Systems, Curtin University of Technology, Australia*
E-mail: {Elizabeth.Chang, Farookh.Hussain}@cbs.curtin.edu.au
[2] *eXel Lab, Faculty of IT, University of Technology, Sydney, Australia*
E-mail: tharam@it.uts.edu.au

Abstract

Trust and trustworthiness plays a major role in conducting business o the internet in service-oriented environments. In defining Trust for service-oriented environments, one needs to capture the notation of service level, service agreement, context and timeslots. The same applies for reputation which is the opinion of the third party agents which is used in determining the trust and trustworthiness. Because of the complexity of the issues, and the fact that the Trust and Reputation are essentially concerns with the relationships, it is important to clearly define the notion of the trust relationships and notion of the reputation relationships. In this paper, therefore, we clearly these definitions and we introduce a graphical notation for representing these relationships.

1. Introduction

The advent of the Internet and Web provide connectivity and information richness over great distances at any time. This has created a dynamic, open and convenient environment for social and business development. It not only provides the opportunity for new entrepreneurial endeavours utilizing the Web, but also opens up new opportunities for the old, static, closed, locally based business to adopt a new business paradigm and new organizational forms. The Internet has also opened up modes of interaction and dynamic organizational configurations that were previously inconceivable within a wide array of human and business activities. However, these have also introduced challenges. Thus business or social interaction on the Internet cannot rely on the usual physical, facial and verbal cues to reach a judgement as to the trustwothiness of the parties. In addition, in the case of the purchase of physical goods over the Internet, we have no direct physical, sensory contact with the specific product and are reliant solely on the promise of the seller. We are being put in the position of 'buying a pig in a poke', rather than being able to 'squeeze the tomatoes' to determine their firmness. There could, in some cases, be difficulties ensuring the purchaser pays for the goods. These factors and several others, when taken together, create the imperative for being able to make judgements within such an environment about the other parties' trustworthiness and capability to provide the service at a specific level of quality. Through adopting new trust technology a platform for both consumers and businesses to learn from each other can be created. Thus, real business value, indeed consumer confidence, true product and service reputation could become a reality in the virtual word.

In this paper, we study why Trust is important and make clear distinctions between the concepts of trust and security. We also provide approaches for determining Trust and reputation. In addition we define the notions of Trust and Reputation Relationships and provide a diagrammatic approach to representing them.

2. Why Trust?

All In recent times, we have seen an increasing number of people carrying out a myriad of different activities on the Internet. These range from writing reports to looking at news, from selling a car to joining a club, from the purchase of goods (e.g. Amazon.com) to the purchase of services (e.g. Priceline.com for travel arrangements), from entertainment (music or games) to research and development (information surfing), from private resource utilization (Grid computing) to remote file sharing (peer to peer communication), from shopping at the mall (BizRate.com) to bargaining in virtual markets (eBay), from e-bill to e-pay, from the virtual community to

Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05)
0-7695-2316-1/05 $20.00 © 2005 IEEE

virtual collaboration, from e-governance (e-administration) to mobile commerce (Stock Trading), from e-education (cyber-university) to e-learning (getting an MBA online), from e-manufacturers (remote control production) to e-factory (e-products), from off-shore development (business expansion) to outsourcing (such as IT), from e-warehouse (warehouse space booking) to e-logistics (goods shipping orders), and limitless other possibilities.

Transactions have moved away from less face-to-face encounters to more on the Internet. The infrastructure for the above business and information exchange activities could be a client-server, peer-to-peer (P2P), or mobile networks. Most times, users on the network (the customer or business providers), carry out interactions in one of the following forms:

- Anonymous (No name is to be identified in the communication)
- Pseudo-anonymous (Nick names are used in the communication)
- Non-anonymous (Real names are used in the communication)

In such distributed, open and often anonymous environments, *fraudulent* or *incomplete practice* could occur where the seller or business provider or buyer (the agents on the network) does not behave in a manner that is mutually agreed or understood, especially where terms and conditions exist. This could take several forms:

(a) The *seller* or *service provider* only delivers part of the service or partial promises, or is inconsistent in delivering the goods or services e.g. sometimes delivers and sometimes does not deliver or cannot deliver or never delivers what was promised or advertised;
(b) The *customer* or user may always be negative and disruptive of the business, or gives false or faulty credit details;
(c) The provider provides a *service*, however it is not up to an acceptable standard;
(d) The seller's *product* is not of a good quality.

Trust and *Trust Technology* have come into the picture for the virtual environment recently to give an online user the sensation of being able to 'squeeze the tomatoes before you buy' or opinions before you make a decision. It boosts consumer confidence and helps facilitate judgements about business reputations. In other words, you feel confident to pay for a service or product because you trust the seller's reputation or the quality of products (goods) or services. This helps mitigate the risk in the business transaction. On the other hand, *sellers* or *service providers* can learn about users and customers through trust technology so that they can improve on-demand service that better meets customer needs. Trust technology such as trustworthiness systems, or rating systems, or recommender systems already exist on the Web. For example e-Bay, Amazon, BizRate and CNet already have some rudimentary versions of trust technologies. Regardless of the fact that these examples of the use of the technology only provide some basic functions, trust technologies are becoming more and more popular and providing a convenient tool to simulate the social trust and recommendation experience for online users.

3. Trust and Security

Trust and security are not the same thing in the world of e-Commerce. Unfortunately a variety of uses, particularly of the term 'trust', could lead to some confusion. In this section, we clearly distinguish trust and security and when they could be synonymous and when they are not.

Security focuses on protecting users and businesses from anonymous intrusions, attacks, vulnerabilities etc., while ***Trust*** helps build consumer confidence and a stable environment for customers or businesses to carry out interactions and transactions with a reduction in the risk associated with doing these in a virtual world, thus allowing one to more fully reap the possible rewards of the increased connectivity, information richness and flexibility.

The dynamic, open and convenient Web environment not only boosts business potential and the economy but also creates concerns of security, trust, privacy and risks. If these issues are not dealt with in a timely fashion, they could hamper business development utilizing the Web. As mentioned earlier, security issues can affect communication, infrastructure, servers, client browsers, e-products, e-services, software, hardware, electronic documents, business transactions, and organizational backend databases. We need to prevent hackers, attackers, unauthorized individuals, and malicious users or servers from taking advantage of honest online users, from damaging private businesses and also from attacks on non-government organizations.

Security threats and attacks on the Internet include, but are not limited to, the following (Vesna Hassler 2001):

- Eavesdropping - intercepting and reading message intended for other users
- Masquerading - sending/receiving messages using another user's ID
- Message tampering - intercepting and altering messages intended for other users

- Replaying - using previously sent message to gain another user's privileges
- Infiltration - abusing a user's authority in order to run hostile or malicious programs
- Denial of service - preventing authorized users from accessing various resources
- Virus and worms - micro virus or attachment virus, Morris worm, cert/cc)

Security Technologies that are widely available to address these include:

- Encryptions (RSA encryptions, algorithms, keys, encryption standards, etc.)
- Cryptography (hiding messages in text)
- Steganography (hiding messages in pictures or media)
- Secret information sharing (algorithms, symmetric keys)
- Digital signatures and standards
- Authentication (digital certificates, verifying identities, public keys)
- Authorization (controlling access to particular information and resources)
- Data integrity (a receiver can detect if the content of a message has been altered or a receiver can detect it)
- Intrusion detection

Currently, the above mentioned security technologies are sufficiently mature for e-commerce, and most of the technologies are already standardized (Hassler, 2001) .

Security and trust are two distinct concepts. Security provides a safe environment and secure communication along with end user and business protection. Trust is the belief or faith that a person or agent has in another person or agent with respect to certain activities at a given time. In order to acquire trust in another entity over the anonymous distributed network, security establishing mechanisms may be necessary to provide sheltered communication or information protection.

Trust, Trustworthiness and Reputation are innovative technologies re-shaping the world of e-commerce. Many of the largest commerce websites and organizations are already adopting these technologies. They help business providers learn from their customers and help the customers to find the best deals available and understand the risks associated with a transaction with a particular supplier. The concepts of 'Trusted Computing', 'Trusted Network', Trusted Communication', 'Trusted Agents', 'Trusted …' etc, are related to security issues, security mechanisms, security technology and security services. All topics of security study and research are directed towards providing a secure and tamper free environment, or network or communication. In this context, 'trust' is synonymous with 'secure', which is tied to 'security'. However, this is not the same in the business paradigm.

Trust is a belief of confidence or a feeling of certainty that one person has in another person or thing that he/she is interacting with. Everyone or every organization wants assurance, certainty and confidence about what they do and what they will receive. In the business world, trust is especially tailored for ensuring honest dealings, quality of products or services and that is usually related to mutual agreements and understandings. When we discuss trust in a social or economic context, there is a limited relationship with security. The motivation of trust technology is to help build business reputation, consumer confidence, fair trading, and mutual relationships. This paper is about Trust in Business and specifically focuses on trust technology, trust establishment, trust level measurement and prediction and trust relationship development. *Security* can be used to support *Trust*, through providing a secure trusted environment, secure network and secure communication, so that trusted business transactions can take place. However, building trust in social and economic environments also helps to reduce aspects of *Security Risk*.

4. Trust. Trustworthiness and Reputation in Literature

In computing literature, Marsh (1994) was the first person to introduce the concept of *trust* in distributed artificial intelligence. Marsh (1994), Rahman (2003) and several other researchers in the area of computing use the definition given by Gambetta (1990) who defines trust as: '*…trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own actions'.* The above definition classifies trust as a probability. However, one may note that trust is also a belief or confidence and sometimes we do explicitly know what we trust, in a particular context and at a particular time. Wang (2003) defines *trust* as: '*…an Agent's belief in another Agent's capabilities, honesty and reliability based on its own direct experiences'.* The above definition ties trust to direct interaction only. Note that most of the above definitions concentrate on the action or behavioural aspects of trust while some cover the context dependent nature of trust. However, there are

many other aspects related to the concept of trust. These include the dynamic nature of trust (the value of trust changes as time passes) and the anticipated behaviour of the trusted party which would influence the trust. There are also psychological factors for the trusting party and the trusted party, as well as the Agent's calibre (knowledge, capability and professional qualities) that need to be taken into consideration.

Reputation has been widely used in different disciplines like sociology, economics (Celentani et al (1966) and Marimon et al (2000)) and psychology (Bromley (1993) and Abelson (1970)). In the area of computing, the concept of reputation has been applied to Multi-Agent Systems (Esfandiari and Chandrasekaran (2003), Yu and Singh (2003), Sabater and Sierra (2003), Pujol et al (2003)). Recently, reputation has attracted the attention of service-oriented networks and e-Business (Abdul-Rahman and Hailes (2000), Cornelli et al (2003), Aberer and Despotovic (2003), Xiong and Liu (2002), Lee et al (2003). Sabater and Sierra (2003) define *reputation* as *"Opinion or view of one about some thing"*. Abdul-Rahman and Hailes (2000) define *reputation* as *"an expectation about an agent's behavior based on information about or its past behavior"*. Mui et al (2003) define *reputation* as "*perception that an Agent creates through past actions about its intentions and norms*". Note that the above definitions have not considered the time factor, the context factor and that there is no mention of who are eligible to vouch for an agent's reputation. The reputation of a given agent has a time frame (time slot). The reputation may or may not be the same at the next instance of time. Context is important when defining reputation, e.g., a university may have a good reputation in Engineering, but not in Medicine. Miztal (1996) defines **reputation** as "*Reputation helps us to manage the complexity of social life by singling out trustworthy people-in whose interest it is to meet promises* ". This definition of reputation focuses on the purpose of reputation as a means of finding trustworthy people. Although this is correct, it does not mention whose reputation is under consideration, at what given point of time, in what context and more importantly who are eligible to vouch for the reputation.

5. Trust Definition

Trust Definition: In Service-oriented network environments, we define **Trust** as *the belief t*hat the *Trusting Agent* has in the *Trusted Agent's willingness* and *capability to deliver a quality of service* in a given *context* and in a given *Timeslot.*

The terms 'belief', 'Trusting Agent' and 'Trusted Agent', 'willingness', 'capability', 'delivery', 'mutually agreed service', 'context', 'Timeslot' are essential when defining trust. These terms can be regarded as the building blocks of trust .Some of these terms are explained below:

We state that trust is context dependent because the belief that the Trusting Agent has in the Trusted Agent, in a given context, will not necessarily be the same in another context. The term *willingness* captures and symbolizes the Trusted Agent's will to act or be in readiness to act honestly, truthfully, reliably and sincerely in delivering on the mutually agreed behaviour.The willingness of a Trusted Agent to deliver on the mutually agreed behaviour is one of the two characteristics that the Trusting Agent can make a qualitative inference about from the actual behaviour of the Trusted Agent in its interaction. The other characteristic that the Trusting Agent can make a similar inference about is the *capability* of the Trusted Agent.

The term *capability* captures the talent, competence, aptitude and ability of the Trusted Agent in delivering on the mutually agreed behaviour .If the Trusting Agent has low trust in the Trusted Agent, it signifies that the Trusting Agent believes that the Trusted Agent does not have the capability to deliver on the mutually agreed behaviour.

Trust is dynamic and as such the amount of trust changes as time passes. This dynamic nature is due to the following three reasons: a) The Trusting Agent can get a better idea of the capability and willingness of the Trusted Agent to deliver on the mutually agreed service in a given context by engaging in *further dealings* with the Trusted Agent, b) The capability or the willingness of the Trusted Agent to deliver on the mutually agreed behaviour in a given context *may vary over time*, c) Getting recommendations from other Agents about the Trusted Agent in a given context may have an impact on the trust which the Trusting Agent has in that context. Upon querying other Agents about the Trusted Agent, the Trusting Agent can get a better idea of the willingness and capability of the Trusted Agent to deliver on the mutually agreed behaviour in a given context. This may result in a change in the trust that the Trusting Agent has in the Trusted Agent. The term *a given Timeslot*, in the definition of trust, captures the dynamic nature of the trust.

The term *delivery* captures the actual service delivered by the Trusted Agent in the interaction. The delivery of a quality service is a measure of the behaviour of the Trusted Agent. The Trusted Agent in

the interaction may or may not deliver the mutually agreed service. We refer to the actual service delivered by a Trusted Agent as the *conduct* of a Trusted Agent in an interaction.

Quality of Service (QoS), in a Service-oriented network environment, is defined as the *fulfilment* of the *service agreement* or *mutually agreed service.*

In a service contract or agreement, a service is defined by its context or functions, coupled with the terms and conditions and is normally set by agreement between the service requestor and the service provider. In other words, a service agreement describes a mutually agreed service, and that both customer and service provider have agreed upon all the terms and conditions. Quality of service can then be measured against the fulfilment of the mutually agreed service as specified in the service agreement. A service in the service agreement is clearly defined as to have a clear context or functions and a set of terms and conditions that are tailored to the customer's requirements.

6. Trust Relationships

Trust is realized by the concept of a **Trust Relationship**. Without a relationship, trust has no meaning. However, a relationship is conditioned by the parties. Without the involvement of parties, there can be no Trust Relationship. For the purposes of this discussion, we will define a trust relationship as a *bond* or *association* between a Trusting Agent and a Trusted Agent. Each relationship that the Trusting Agent has with the Trusted Agent is coupled with a numeric value that denotes the *strength* of the trust relationship in a particular context.

The trust relationship between two Agents is always **unidirectional**. If we assume the Trusting Agent is A and the Trusted Agent is B, the trust value assigned to the relationship is from Agent A to Agent B. The trust value is assigned in **one direction** from the Trusting Agent to the Trusted Agent on a scale of 0 to 5. This is due to the fact that, in a given context, e.g., borrowing a credit card, the level of trust Agent A has in Agent B may be different from the level of trust Agent B has in Agent A. In the Service-oriented business world, it is very important to recognise the fact that the trust measure is unidirectional from the Trusting Agent to the Trusted Agent.

A Trusting Agent may have several Trusted Agents; this will result in multiple trust relationships. They may be in the same or different contexts. However, each individual relationship will result in an individual trust value.

At any given Timeslot, multiple trust relationships can exist between multiple Agents or between the same Agents where an additional association exists between them. Also for the same *contex*t, multiple relationships may be formed between multiple Agents.

In a relationship between a Trusting Agent and a Trusted Agent, there is always a *Trust Value* that expresses the strength of the relationship (or the degree of trust) from the Trusting Agent to the Trusted Agent.

- There is a M:M (Many-to-Many) relationship between Trusted Agent and Trusting Agent.
- The Trust Value is unique in each of the trusted relationships, and the combination of Trusting Agent and Trusted Agent is unique.
- For a given Trusting Agent and a given Trusted Agent engaged in a given Trust Relationship there can be **only one Trust Value**. Therefore, there is a M:M:1 (Many-to-Many-to-One) relationship between Trusting Agent, Trusted Agent and Trust Value.

A Trust Relationship is determined by a particular *time* and in a given *context*. Each of the relationships has to be associated with a Trust Value to reflect the strength of the bond.

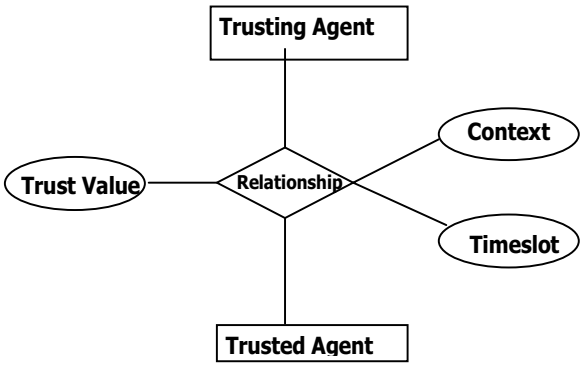

Figure 1 (a): Context and Time Dependence in a Trust Relationship

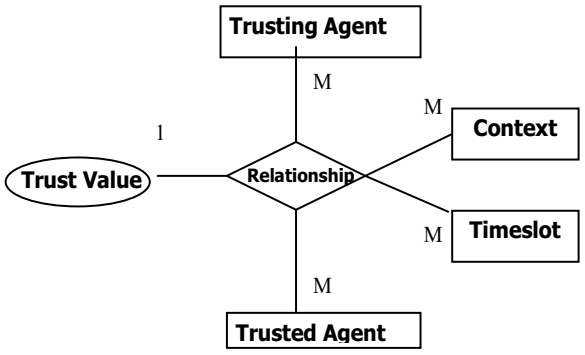

Figure 1 (b): Context and Time Dependence in a Trust Relationship with Cardinality

The *association* between the Trusting Agent and the Trusted Agent is defined as the actual interaction between two Agents with a common need or which shares a common interest in a particular Timeslot.

There are three scenarios that form the association, namely:

- Association through direct personal contact or interaction;
- Association through third party introduction;
- Association through reviewing ones history record.

These three scenarios are called the *Initiation of the relationship*. In other words, they describe how the association is formed.

We define the *initiation of the trust relationship* as a type of initial introduction that results in an association or a relationship and that *provides methodologies* for *calculating or deriving* the trust value. There are *mainly three* different types of initiation as mentioned above and depicted in Figure 2 namely Direct Interaction; Reputation and History.

*Initiation of the relationship by direct interaction***:** This is started by direct contact between the Agents without any mediator or without the parties knowing each other upfront or from any recommendation. The relationship generally begins from a mutual sense of requirement. *Initiation of the relationship by Recommendation* (also known as *introduction or obtaining reputation*)**:** This relationship is begun by a third party mediator who provides an introduction or recommendation. *Historical* (or past knowledge) review or look at past records may result in a new or renewed trust relationship. Historical data could be obtained from the trusting agent's own history repository (past personal interaction data).

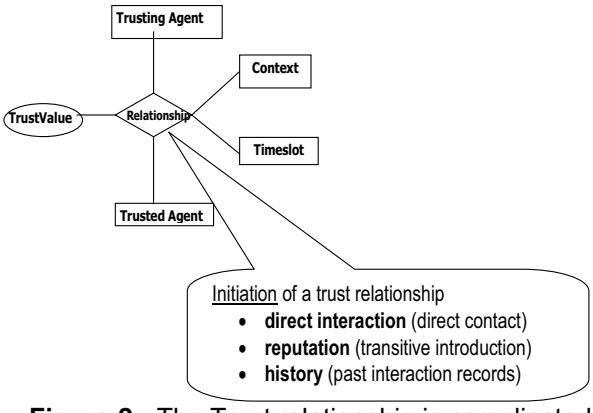

Figure 2 : The Trust relationship is complicated as you need to consider the *initiation* of the relationship

7. Reputation

Definition: In service-oriented environments, we define reputation as the Third Party Recommendation Agents' Opinions in response to the reputation query for the trustworthiness of the Trusted Entity (such as Trusted Agent or Quality of the Product or Service etc).

Fundamentally, **reputation** is about the trustworthiness of a *Trusted Entity (such as Trusted Agent* or quality of *Product* and services) and is the Opinion of the Recommendation Agents or the third party agents and it is not assigned, but only requested by the Trusting Agent.

The four keywords in the reputation definition:

1) *Reputation*, which represents the Trustworthiness of the *Trusted Entity from Third Party Agents point of view.*
2) *Recommendation or Opinion*.
3) *Recommendation Agent w*hich is a subset of the *third party agents* who offer to share their opinions.
4) *Reputation Query,* which is the query made by the Trusting Agent.

In service-oriented network environments, all other agents, with the exception of the Trusting Agent and the Trusted Agent in a given relationship, are referred to as *Third Party Agents*. They could be non-anonymous agents, pseudo-anonymous agents and anonymous agents.

In service-oriented network environments, Third Party *Recommendation Agents* are Third Party Agents who give a Recommendation, feedback or opinion. Not all the third party agents give Recommendations; therefore, Third Party Recommendation Agents are a subset of the Third Party Agents.

There are four types of *Third Party Recommendation Agents* from the Trusting Agent's point of view, namely:

(a) The *Known Agents* - agents who are known by the Trusting Agent (including trusted and un-Trusted Agents). They are non-anonymous or pseudo-anonymous agents.
(b) The *Referred Agents* - agents who are not known by the Trusting Agent only by references provided by *known agents.* They are non-anonymous or pseudo-anonymous agents.
(c) The *Unknown agents* - agents with no referral or direct interaction with the Trusting Agent. They are anonymous agents.
(d) The *Malicious agents* - agents who intentionally disrupt the business and services, and are discovered by the Trusting Agent though

interaction. They could be anonymous, non-anonymous or pseudo-anonymous.

A *Reputation Query* is the enquiry made in a specific *Context* regarding a Trusted Agent, product, or service. It may include Context ID, Context Description and Context Time, etc. The term Reputation Query is also interchangeable with "Asking Opinions", "Getting Recommendations", 'Calling for Referees", or "Invitation for Feedback".

8. Reputation Relationship

Definition: The nature of the *Reputation Relationship* in a service-oriented environment is defined as the relationship between Trusting Agents, Third Party Agents, and Trusted Entities when the reputation query is made. The *Recommendations* are presented by third party agents and the *reputation value* is calculated. It involves three relationships, known as reputation query relationship, Recommendation relationship and third party trust relationship.

The nature of the *Reputation relationship* has the following complexity, namely:

1) It involves three entities, namely: Trusting Agent, Third Party Agents and Trusted Entity. This is a major difference between *Reputation relationship* and the *Trust Relationships*, is the involvement of the *Third Party Recommendation Agent*.
2) It involves three relationships, reputation query, Recommendation and third party trust relationships.
3) The Trusting Agent may not know all the agents who give Opinions or feedback.
4) There may be malicious agents existing in the network.
5) There may be malicious Opinions from someone the peer trusts.
6) How do we trust the third party agents?
7) How do we know the Opinions are correct or not?

8.1. Recommendation Relationship

Definition: *Recommendation Relationship* is defined as the relationship between the Trusting Agent and the third party recommendation agent. This relationship represents the trustworthiness of the *Third Party Agent* namely its willingness and capability to give a *Correct Recommendation* or *Opinion* in a particular *context* and a particular *time* and is assigned by the Trusting Agent.

The recommendation relationship is important to address the trustworthiness of Third Party Agents in giving the correct Recommendation. In other words, the Recommendation relationship depicts whether the 3rd party will give a correct Recommendation or not.

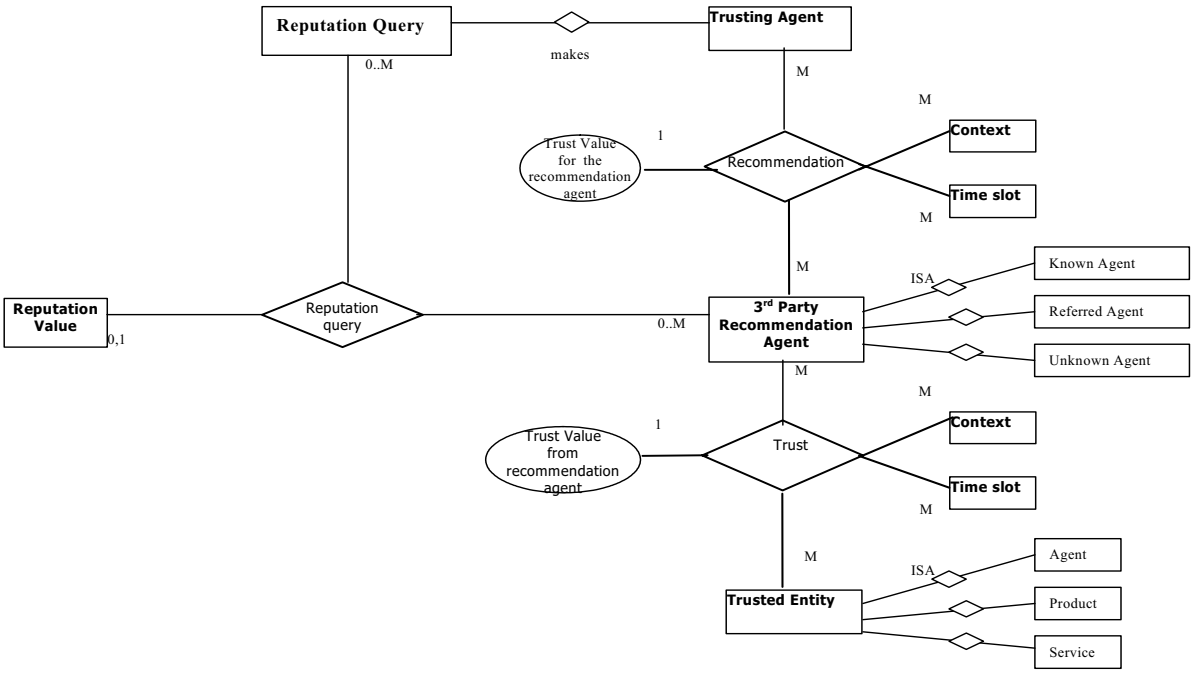

Figure 4: The low level view of the Reputation Relationship

8.2. Third Party Trust Relationship

Definition: The *third party trust relationship* is defined as the relationship between the third party agent and the Trusted Entity. This relationship is a form of Trust Relationship explained in Chapter 2, except the Trusting Agent is a Third Party Agent.

There are two differences between this *Third Party Trust Relationship* and the Trust Model earlier, namely:

1) In this case the Third Party Recommendation Agents as the Trusting Agent,
2) Here the trusted entity implies trusted agent, or product or service etc. Whereas in the Trust Model, only Trusted Agents were involved.

8.3. Reputation Query Relationship

Definition: The *Reputation Query Relationship* is defined as the relationship between the Reputation Query, Third Party Recommendation Agents and the Reputation Value. The relationship will result in generating a reputation value that is recommended by the Third Party Agent.

The reputation relationship is built around the Third Party Agents who give Recommendations or Opinions to the Trusting Agent about the trustworthiness of the Trusted Entity. They are involved in three relationships, namely Reputation Query Relationship, Recommendation Relationship and 3rd Party Trust Relationship, and their trustworthiness is assessed by the Trusting Agent based on their willingness and capability to give the right information or correct Opinion or Recommendation in a given context and time slot.

9. Trustworthiness

Definition: Trustworthiness is defined as an estimate of the level of trust that the Trusting Agent has in the Trusted Agent. The Trustworthiness scale system provides the reference standard for trustworthiness measurement and trustworthiness prediction. It quantifies the trust values and rates the trust in Service-oriented networks.

The term '*an estimate'* refers to trustworthiness which gives *a measure* of the level or the degree of trust. *An estimate* is the result of *a tentative measure*. A tentative measure could be in the form of an expert opinion or appraisal and it is a scientific judgment or prediction. *An estimate* gives an approximate measure against some scale or standard and often, the result is a value.

The term *'the level* of trust' determines the *amount* of trust that the Trusting Agent has in the Trusted Agent. It can be represented numerically or non-numerically

If the Trusting Agent has a high degree of trust in the Trusted Agent, then this implies that the Trusted Agent's trustworthiness level is high, i.e., the *amount* of trust that the Trusting Agent has assigned to the Trusted Agent is high on the Trustworthiness Scale. Conversely, if the assigned Trustworthiness level is low, it means that the Trusting Agent has little trust in the Trusted Agent.

The level of trust represented by the Trustworthiness is *unidirectional* from the Trusting Agent to the Trusted Agent and it depends on the context and time, as was the case with Trust.

'*A scale system*' is defined as a measurement system which can be used to determine the level of trust. The scale system can have either numeric measures or non-numeric measures. We define the *numeric measure* of a trust level as an assessment of a trust relationship expressed in terms of an integer or a real number. We define the non-numeric measure of a trust level as a valuation of a trust level expressed neither in terms of an integer nor in terms of real numbers, but as lexicons such as Very Trustworthy or Untrustworthy.

'*Trustworthiness Measure*' is defined as an estimate of the level of trust or the trustworthiness value assigned to the Trusted Agent *AFTER* a business service interaction over the distributed Service-oriented environment.

'*Trustworthiness Prediction*' is defined as the initial trust value assigned to the Trusted Agent *BEFORE* a business service interaction over the distributed Service-oriented environment.

Trustworthiness is *a measure* that *determines* the *amount of trust* that the Trusting Agent has in the Trusted Agent. It provides a 7-level trustworthiness scale system and helps to quantify the trust values. *Quantify,* here, means to calculate the trust value in order to determine the corresponding trustworthiness levels.

Trustworthiness helps in the rating of trust by numerically quantifying the trust values and qualifying the trust levels non-numerically. Here, the term *qualify* means to give a specific meaning to the level that is derived.

In other words, the Trustworthiness measurement system provides a *Trust Rating*, which is a non-numerical description of trust levels and if the *amount of trust* is high (numerical rating) then the *trust rating* is also high (non-numerical rating).

'Rating the trust' is the process of using the trustworthiness scale (numerical and non-numerical ratings) to qualify the trust level to the Trusted Agents in the network.

We can represent the *seven discrete trustworthiness levels* and their semantics visually using a system of stars and half stars. Table 1 below illustrates the visual scale.

Table 1: *Seven levels* of trustworthiness and a corresponding visual representation

Trustworthiness Level	**Semantics** (Linguistic Definitions)	**Trustworthiness Value** (User defined)	**Visual Representation** (Star Rating System)
Level -1	Unknown Agent	x = -1	Not displayed
Level 0	Very Untrustworthy	x = 0	Not displayed
Level 1	Untrustworthy	$0 < x \leq 1$	From ½★ to ★
Level 2	Partially Trustworthy	$1 < x \leq 2$	From ★½★ to ★★
Level 3	Largely Trustworthy	$2 < x \leq 3$	From ★★½★ to ★★★
Level 4	Trustworthy	$3 < x \leq 4$	From ★★★½★ to ★★★★
Level 5	Very Trustworthy	$4 < x \leq 5$	From ★★★★½ to ★★★★★

We note that Level 0 and Level -1 are labelled 'not displayed' or 'normally not displayed'. It is recommended that these levels not be displayed via Service-oriented networks. This is because customers or consumers would only be interested in doing business transactions with a business provider that can be trusted to some degree. On the other hand, from the business provider's point of view, it is a waste of web space or time for them to advertise businesses or business services that are unknown or untrustworthy.

The *Trustworthiness Scale* in a Service-oriented network environment includes 7-levels and associated numerical and non-numerical measures.

The Trustworthiness Scale provides a standard measuring system that allows us to measure the amount of trust that the Trusting Agent has in the Trusted Agent or helps the Trusting Agent to assign trust levels to the Trusted Agent.

The *numeric scale* of trustworthiness can represent *a measure* of trust by ascertaining *a value* and expressing it in terms of *an integer* or *a real number* (e.g. 5, 8.9, 100%).

The *non-numeric scale* of trustworthiness can represent *a rating* of trust by ascertaining levels, grades or rankings and expressing these not in terms of integers nor in terms of real numbers, but in *categorical terms* such as *very trustworthy* or *5 stars*.

9.1. Trustworthiness of the Trusted Agent

Any *Third Party agents* could be a *Trusting Agent* and if the *Third party agent* had a direct interaction with the Trusted Agent, there should be a trustworthiness value assigned by the *third party agent* to the Trusted Agent. However, when he/she vouches his/her Opinion about trustworthiness of the Trusted Agent, this *trustworthiness value* becomes a *reputation* value.

In other words, Trustworthiness assigned by the Trusting Agent to the Trusted Agent, becomes reputation of the Trusted Agent, when the Trusting Agent vouches or conveys this to other agents.

9.2. Trustworthiness of the Recommendation Agents in giving the correct Opinion

The Trusting Agent and assign a Trustworthiness Level to the Third Party Recommendation Agent based on the Agent's willingness and capability in giving the correct Opinion to the Trusting Agent. We can assign one of the following levels to the Recommendation Agents.

9.3. Trustworthiness of the Opinion

To validate the trustworthiness of the Opinion, we look at the context of the Opinion or the Recommendation, when compared to what we know or trust about the Recommendation Agent for a given context. We therefore assign one of the following levels to the trustworthiness of the Opinion

10. Conclusion

In this paper we examine the ideas of trust and reputation from a business perspective. We distinguish between Trust and Security. We define the concepts of Trust, Trustworthiness and Reputation within a service oriented environment. We next define the ideas of Trust Relationship and Reputation Relationship and provide a Graphical notation for representing these.

11. References

[1] Aberer, K. & Despotovic, Z., (2003), *Managing Trust in an Agent-2-Agent Information System*, Available: http://citeseer.nj.nec.com/aberer01managing.html

[2] Burton, K.A., (2002), *Design of the OpenPrivacy Distributed Reputation System*, Available: http://www.Agentfear.org/papers/openprivacy-reputation.pdf.

[3] Chen, R. & Poblano, Y.W., (2003), *A distributed Trust Model for Agent-to-Agent Networks*, Available: http://www.jxta.org/docs/trust.pdf (20/9/2003).

[4] Cornelli, F., Damiani, E., Vimercati, S., De Capitani di Vimercati, Paraboschi, S. & Samarati, P., (2003), *Choosing Reputable Servents in a P2P Network*, Available: http://citeseer.nj.nec.com/cache/papers/cs/26951/http:zSzzSzseclab.crema.unimi.itzSzPaperszSzwww02.pdf/choosing-reputable-servents-in.pdf (20/9/2003).

[5] Dragovic, B., Kotsovinos, E., Hand, S. & Pietzuch, P., (2003), 'Xeno trust: Event based distributed trust management', *Proceedings of DEXA'03*, 1st ed, IEEE, Los Alamitos, California, Prague, Czech Republic, pp. 410-414.

[6] Gambetta,D., (1990), *Can we trust trust?*, Available: http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

[7] Hartman, F., (2003), 'The role of trust in successful system development and deployment', *Proceedings of IEEE Conference on Industrial Informatics 2003*, Banff, Canada.

[8] Dillon, T.S., Chang, E. & Hussain, F.K., (2004), 'Managing the dynamic nature of trust', *IEEE Transaction of Intelligent Systems*, Sept/Oct 2004, vol. 19, no. 5. pp. 77-88

[9] Hussain, F., Chang, E. & Dillon, T.S., (2004), 'Classification of trust relationships in peer-to-peer (P2P)', *Proceedings of the Second International Workshop on Security in Information Systems.*

[10] Kamvar, S.D., Schlosser, M.T. & Garcia-Molina, H., (2003), *The EigenRep Algorithm for Reputation Management in P2P Networks*, Available: http://citeseer.nj.nec.com/kamvar03eigentrust.html

[11] Marsh, S., (1994), *Formalizing Trust as a Computational Concept*, Ph.D., University of Sterling.

[12] Ooi, B.C., Liau, C.Y. & Tan, K.L., (2003), *Managing Trust in Agent-to-Agent Systems Using Reputation-Based Techniques*, Available: http://citeseer.nj.nec.com/cache/papers/cs/30109/http:zSzzSzwww.comp.nus.edu.sgzSz~ooibczSzwaim03.pdf/managing-trust-in-Agent.pdf

[13] Rahman, A.A. & Hailes, S., (2003), *Supporting Trust in Virtual Communities*, Available: http://citeseer.nj.nec.com/cache/papers/cs/10496/http:zSzzSzwww-dept.cs.ucl.ac.ukzSzcgi-binzSzstaffzSzF.AbdulRahmanzSzpapers.plzQzhicss33.pdf/abdul-rahman00supporting.pdf.

[14] Rahman, A.A. & Hailes, S., (2003), *A Distributed Trust Model*, Available: http://citeseer.nj.nec.com/cache/papers/cs/882/http:zSzzSzwww-dept.cs.ucl.ac.ukzSzcgi-binzSzstaffzSzF.AbdulRahmanzSzpapers.plzQznspw97.pdf/abdul-rahman97distributed.pdf (5/09/2003).

[15] Rahman, A.A. & Hailes, S., (2003), *Relying On Trust To Find Reliable Information*, Available: http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/dwacos99.pdf

[16] Ratnasingham, P., (1998), 'The importance of trust in the digit network economy', *Electronic Networking Applications and Policy*, vol. 8, pp. 313-321.

[17] Singh, A. & Liu, L., *TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P systems*, Available: http://www.cc.gatech.edu/~aameek/publications/trustme-p2p03.pdf (11/10/2003).

[18] Wang, Y. & Vassileva, J., (2003), *Trust and Reputation Model in Agent-to-Agent Networks*, Available: www.cs.usask.ca/grads/yaw181/ publications/120_wang_y.pdf

[19] Wang, Y. & Vassileva J., (2003), *Bayesian Network Trust Model in Agent-to-Agent Networks*, Available: http://bistrica.usask.ca/madmuc/Pubs/yao880.pdf

[20] Xiong, L. & Liu, L., (2003), *A Reputation-Based Trust Model for Agent-to-Agent eCommerce Communities*, Available: http://citeseer.nj.nec.com/xiong03reputationbased.html.

[21] B.Miztal 1996, Trust in Modern Societies, Polity Press, Cambridge,MA.

[22] Babak Esfandiari, Sanjay Chandrasekaran, On How Agents Make Friends: Mechanisms for TrustAcquisition,Available: [http://citeseer.nj.nec.com/cache/papers/cs/26840/http:zSzzSzwww.sce.carleton.cazSznetmanagezSzpaperszSztrustworkshop.pdf/on-how-agents-make.pdf] (10/10/2003).

[23] Bin Yu, Munindar P. Singh, An evidential Model of Distributed Reputation Management, Available: [http://www-2.cs.cmu.edu/~byu/papers/p406-yu.pdf] (99/09/2003).

[24] Bromley, D. B. 1993, Reputation,Image and Impression Management, John Wiley&Sons.

[25] Fabrizo Cornelli, Ernesto Damiani, Sabrina De Capitani di Vemarcati,Stefano Paraboschi,Pierangela Samarati 2003, Choosing Reputable Servants in a P2P Network, Available: [http://citeseer.nj.nec.com/cache/papers/cs/26951/http:zSzzSzseclab.crema.unimi.itzSzPaperszSzwww02.pdf/choosing-reputable-servents-in.pdf] (10/10/2003).

[26] Abelson, M. K. a. H. 1970, Persuasion,how Opinion and attitudes are changed, Crosby Lockwood &Son.

[27] Jordi Sabater, Carles Sierra, REGRET: A reputation model for gregarious societies, Available: [http://citeseer.nj.nec.com/cache/papers/cs/22333/http:zSzzSzwww.iiia.csic.eszSzReportszSz2000zSz2000-06.pdf/sabater00regret.pdf] (15/09/2003).

[28] Joseph M.Pujol, Ramon Sanguesa, Jordi Delgado 2003, Extracting Reputation in Multi Agent Systems by Means of Social Network Topology, Available: [http://citeseer.nj.nec.com/pujol02extracting.html] (09/10/2003).

[29] Karl Aberer, Zoran Despotovic, Managing Trust in a Agent-2-Agent Information System, Available:

[http://citeseer.nj.nec.com/cache/papers/cs/26315/http:zSzzSzwww.p-grid.orgzSzPaperszSzCIKM2001.pdf/aberer01managing.pdf] (10/10/2003).
[30] Li Xiong, Ling Liu 2002, Building Trust in Decentralized Agent-to-Agent Lizlectronic Communities, Available: [http://citeseer.nj.nec.com/cache/papers/cs/26940/http:zSzzSzdisl.cc.gatech.eduzSzAgentTrustzSzpubzSzxiong02building.pdf/xiong02building.pdf] (10/04/2003).
[31] Lik Mui , Mojeh Mohtashemi, Ari Halberstadt 2002, A Computational Model of Trust and Reputation, Available: [http://www.cnn.com/2002/WORLD/europe/10/04/world.cities/] (10/10/2003).
[32] Marco Celentani, D. Fudenberg, David K.Levine , Wolfgang Pesendorfer 1966,
[33] Maintaining A Reputation Against A Long-Lived Opponent, Available: [http://citeseer.nj.nec.com/cache/papers/cs/25188/http:zSzzSzlevine.sscnet.ucla.eduzSzpaperszSzedit9.pdf/celentani66maintaining.pdf] (10/09/2003).
[34] Ramon Marimon, J. P. Nicolini, Pedro Teles 2000, Competetion and Reputation, Available: [http://www.utdt.edu/departamentos/economia/pdf-wp/WP002.pdf] (2004).
[35] Seungjoon Lee, Rob Sherwood, Bobby Bhatacharjee 2003, Cooperative Agent Groups in NICE, Available: [http://citeseer.nj.nec.com/cache/papers/cs/27074/http:zSzzSzwww.ieeeinfocom.orgzSz2003zSzpaperszSz31_03.PDF/lee03cooperative.pdf] (30/10/2003).