DEAKIN UNIVERSITY

Risk and Trust Management for Online Distributed System

by

Soon Keow Chong
Bachelor of computing (Honours)

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Deakin University

August, 2012

DEAKIN UNIVERSITY

ACCESS TO THESIS - A

I am the author of the thesis entitled “Risk and Trust Management for Online Distributed System” submitted for the degree of “Doctor of Philosophy”

This thesis may be made available for consultation, loan and limited copying in accordance with the Copyright Act 1968.

'I certify that I am the student named below and that the information provided in the form is correct'

Full Name .... Soon Keow Chong...................... ....

Signed .... Signature Redacted by Library ....

Date...............................24th August 2012...

DEAKIN UNIVERSITY

CANDIDATE DECLARATION

I certify that the thesis entitled " Risk and Trust Management for Online Distributed System" submitted for the degree of "Doctor of Philosophy" is the result of my own work and that where reference is made to the work of others, due acknowledgment is given.

I also certify that any material in the thesis which has been accepted for a degree or diploma by any university or institution is identified in the text.

'I certify that I am the student named below and that the information provided in the form is correct'

Full Name ....Soon Keow Chong.....................................

Signed ....Signature Redacted by Library.........................

Date..................................24th August 2012...............................

Acknowledgements

Firstly, I would like to express my sincere thanks to my supervisor, Associate Professor Jemal Abawajy who offered me this opportunity to pursue my doctoral study at the Deakin University, school of Information Technology. I would like to express my deepest appreciation and sincere gratitude to him for his comments and inputs on this thesis. I would also like to give my warmest thanks to my associate supervisor Dr. Shang Gao. Moreover, I would like to thank Dr Michael Brock, Mr John Cameron, Associate Professor Jo Coldwell-Neilson, Associate Professor Hieu Trinh and Dr Sui Yang Khoo for their time, kindness, encouragement and support during my candidacy.

To my colleagues I would like to thank our research group: Ammar Al azab, Davood Izadi, Hairulnizam Mahdin, Harinda Fernando, Isredza Rahmi A Hamid, Masitah Ahmad, Mohd Farhan Md Fudzee, Mohd Izuan Hafez Ninggal, Shivali Goel, Zulkefli Mohd Yusop for the experience exchanged and encouragement with each other, the laughter we share and our monthly lunch time that I thoroughly treasured.

I feel deeply indebted to my dear husband, without whom I would not have considered to enrol in doctoral research. Without his constant encouragement and assistance throughout all these years, it would have been impossible for me to overcome many difficulties and frustrations especially at the beginning when I had to juggle between family and work. His endless support on both of my life and work has been a great source of inspiration in the completion of this thesis.

I should thank my sons, Timothy, Benjamin and Jonathan, who are the key motivation of my career and life. They bring me a lot of happiness and hopes. Life has become more significant and colourful because of them. Meanwhile, I am so moved by my mother, sisters and brothers, as well as all my sisters-in-law and brothers-in-law, for their constant caring, encouragement and support throughout my life.

Finally, I would like to thank Gateway Church, Ps Phil and Ps Glenys Ward for their prayers and the sharing of wonderful time with my family and their assistance in our life. A lot of other people (too many to mention) played important roles helping me to finish this work. I would like to take this opportunity to express my thanks to them.

Abstract

Online service-oriented distributed systems such as electronic commerce (eCommerce) offer enormous opportunities for online trading while at the same time presenting potential risks. In these systems, trust management has been identified as vital component for establishing and maintaining successful relational exchanges between the consumers and service providers. The purpose of the trust management system is to strengthen the confidence between the service consumers and service providers by promoting an incentive for good behaviour and provision of good quality services while at the same time sanctioning bad behaviour and low quality services. Although trust management system represents an important class of decision support tools that can help reduce risks, there remain many challenges to sufficiently ensure robustness of the trust management system that enable trading partners to select trustworthy service providers, ensuring high quality services and prevent monetary loss. This thesis investigated the problem of strategic manipulation of the feedback attacks and has proposed an approach that makes trust management systems sufficiently robust against feedback manipulation attacks. A multi-attribute risk assessment model is developed. This risk assessment model incorporates various attributes such as transaction costs and trust levels of service providers. The new trust management system enables potential service consumers to determine the risk level of a service before committing to proceed with the transaction. This is useful to online consumers as it allows them to be aware of the risk level and subsequently take the appropriate decisions to minimise potential risks before engaging in risky businesses. The viability of the proposed approach is studied experimentally. The results of various simulation experiments show that the proposed approach is highly effective in identifying falsified and malicious feedbacks. It is also an effective tool to assess the risk level of a service and help minimise potential risks before engaging in risky businesses.

Publications

Journals

1. Chong, Soon Keow and Jemal Abawajy. Enhancing Trust Management System Reliability. Journal of Transactions on Information Forensics & Security. Under review. 6th April, 2012

Conference paper

2. Chong, Soon Keow and Jemal Abawajy the NISS2012: 2012 6th International Conference on New Trends in Information Science and Service Science

3. Chonka, Ashley, Chong, Soon-Keow, Zhou, Wanlei and Xiang, Yang* (2008) Multi-core Defense System (MSDS) for protecting computer infrastructure against DDoS attacks, in Huang, Zhiyi; Xu, Zhiwei; Rountree, Nathan; Lefevre, Laurent; Shen, Hong; Hine, John and Pan, Yi (eds), PDCAT 2008 : Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 503-508, IEEE, Piscataway, N.J.

4. Chong, Soon-Keow, Abawajy, Jemal and Dew, Robert (2007) A multilevel trust management framework, in Lee, Roger (eds), 6th IEEE/ACIS International Conference on Computer and Information Science : (ICIS 2007) in conjunction with 1st IEEE/ACIS International Workshop on e-Activity (IWEA 2007), pp. 776-781, IEEE Computer Society, Los Alamitos, Calif

5. Chong, Soon-Keow and Abawajy, Jemal (2007) Feedback credibility issues in trust management systems, in Kim, Seong-Soo (eds), 2007 International Conference on Multimedia and Ubiquitous Engineering : proceedings : MUE 2007, pp. 387-391, IEEE, Los Alamitos, Calif.

Book Chapter

6. Chong, Soon-Keow and Abawajy, Jemal (2010) Risk-based trust management for e-commerce, in Yan, Zhang (eds), Trust modeling and management in digital environments : from social concept to system development, pp. 332-351, Information Science Reference, Hershey, Pa., USA

Contents

List of Figures

List of Tables

List of Acronyms

eCommerce	Electronic Commerce
B2B	Business-to-Business
B2C	Business-to-Consumer
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
IC3	Internet Crime Complaint Center
DoS	Denial of Service
CF	Collaborative Filtering
BRS	Beta Reputation System
MTMS	Multilevel Trust Management System
ID	identity
DDoS	Distributed Denial of Service
PDA	Personal Digital Assistant

Notation and Symbols

r	Feedback rating
M	Total feedback ratings for a given product /service
f_v	Rating frequency
∂	Weight given to a rating differences
β	Weight given to low value transaction rating
λ	Weight given to rating frequency
$\aleph\vartheta$	Scale factor for rating submission interval
t_i	Total number of submission of a service
$\mathbb{N}$	A scale factor for transaction value
$\mathbb{H}$	A scale factor for frequency
Δt	Difference between the current time and the recording time of the rating r_i
Ω	Difference between a rating submitted by a buyer and the threshold set for a service
b	Buyer
s	Seller
$\mathfrak{M}$	Suspicious rating
W	Window size
τ	Aging factor
p	product/service
t	Time
p_m	is a rating submit by participant m at a time for service P

v_i	Feedback value
T_i	Trust Value
R	Ratings
Cr_i	Credible rating
t_v	Transaction value
r_i	a rating submitted by a buyer (b_i)
b_i	Buyer of product/service (p_i)
r_m	Rating submit by participant m
t_i	Time i when rating submitted
$\leq$	Less than or equal to
$\geq$	More than or equal to
Σ	Summation
e	Exponential function
f_v	Frequency value the value for frequency of ratings submission
n	the total number of ratings submission for a service
t_x	the total number of rating submission by that service x
k	the total number of times of ratings submission
γ	scale factor set by the application
η	the total transaction value submitted by a buyer

μ	percentage of low value transaction
l_v	a set threshold
s_j	trust value of the service providers j
$p^i_{s_j}$	Product i sell by provider s_j
$F^n_{p^i_{s_j}}$	The cumulative feedback rating for the service provider s_j for service Product i
$T_{p^i_{s_j}}$	Trust value of the service providers j on service i
$D_{p^i_{s_j}}$	Purchasing risk value on of the service providers j on service i
$A_{p^i_{s_j}}$	Risk associated with the given product price
$W_{p^i_{s_j}}$	The warranty risk on product i of provider j
wl	The warranty length
wt	The type of warranty coverage
w_1	Scale factor to trust level
w_2	Scale factor to warranty risk
w_3	Scale factor to risk on product price
β_i	Price of a given product i

Chapter 1

Introduction

Distributed service-oriented architectures allow system architects to create a distributed environment in which any number of applications, regardless of geographical location, can interoperate seamlessly in a platform and language neutral manner. This thesis focuses on electronic commerce (eCommerce) online service-oriented distributed systems.

1.1 Trust in eCommerce

eCommerce consists primarily of distributing, buying, selling, marketing, and servicing of products or services over the Internet. It brings many new ways for businesses and consumers to communicate and conduct business on line from anywhere at any time. By offering products and services online, businesses can gain unique benefits such as new customers, cost-effective delivery channel, streamlined enrolment and better marketing through better customer knowledge. Similarly, people can interact with businesses at any hour of the day that is convenient to them. eCommerce offers competitive advantages such as improved productivity and reduced costs. Unfortunately, risk of participating in eCommerce remains big concern. Some of the common issues and concerns for merchants with regard to eCommerce include the need to differentiate legitimate participants from fraudulent users in real time.

Fraud is defined as the use of deception to obtain money or something of value for personal gain or profit. Deceptive and fraudulent activities tend to be increasing in numbers due to the advancement development of online technologies and anonymous nature of eCommerce. There are a number of different types of fraud. The most frequently encountered within the eCommerce industry are criminal activities such as services been paid but were not delivered, credit card frauds etc. Purchase fraud occurs when a criminal approaches a merchant and proposes a business transaction, then uses fraudulent means to pay for it, such as a stolen or fake credit card. As a result, the merchant does not get paid for the sale. On the other hand, a buyer may not receive the goods he already they paid for. Online criminal activities statics show a significant upswing and online fraud is on the rise. The open and anonymous nature of eCommerce presents a potential risk to all the trading partners. According to the Internet Crime watch, online fraud is increasing and costs online businesses millions of dollars. The increased in online fraud is one factor for the erosion of online customers' confidence in eCommerce. However, despite huge amount of efforts and continuous enhancements in security and fraud prevention schemes online trading is not immune to online deception and frauds. This is an indication of why the customers feel uncomfortable engaging in online business transactions. Customers and sellers must trust themselves and the services they are offered. The possibility of dealing with strangers without institutional guarantees such as legal contract significantly increases the risk of such interaction. Therefore, trust is a prerequisite for the continued existence of online eCommerce.

There are many ways of describing trust. We primarily discuss trust in a user or buyer and trust in a seller in an eCommerce environment. Trust is required when there is a decision to be made. Decision making exists in our daily interaction when there are choices to be made. In eCommerce, trust plays a major influence on a customer's decision making behaviour. Trust is often grounded in ongoing relationships between a customer and a seller. For example, a buyer makes a decision in an eCommerce transaction. Usually, the buyer will buy products from a trustworthy seller. He trusts the seller to send him the products and products will also meet his expectations. He also trusts that his personal information is safely kept by the seller and not accessible by others without his authorisation. On the other hand, the seller trusts the buyer to pay for the product. In this situation, if both the buyer and the seller value maintaining the trading relationship they will behave in a trustworthy manner. Thus, trust is used in helping buyers and sellers to make a decision on a transaction.

Trust is also required when in a risky and uncertain environment. Every decision involves a certain amount of risk. Uncertainties may rise to a risky situation when one party is dependent on the behaviour of another party [64]. As a result it is important to pay attention to the customers' risk concern on eCommerce transactions. As customer relationships constitute an important new asset category for eCommerce, trust is a vital factor in determining whether e-business will take place as well as to maintain successful relational exchanges between the business and the consumer [62].Thus, enhancing trust relationship will reduce risk in Internet commerce transactions.

In summary, trust is requires to justify and resolving online transaction risks associated with eCommerce environment. From the eCommerce point of view, trust is a form of risk amelioration strategy. It involves having confidence in the other e-business parties, and hence having an expectation that in an e-business transaction, the trust will not result in a loss. Lack of trust in eCommerce transactions has been identified by researchers as one of the main factors that hamper eCommerce from reaching its full potential [88]. Risk is always present in all businesses and eCommerce is no exception, there are many uncertainties that could diminish potential buyers' confidence [64]. Among the various human factors that affect decision making in an uncertain eCommerce environment, risk and trust are surely crucial ones. Trust is important when decision-makers rely on information from others under conditions of uncertainties, and uncertain matters where it involves risk. Trust and reputation often identify other related entities like fraud and safety. Thus, lack of trust often leads to higher possibility of fraud.

1.2 Current Issues and Research Motivation

Trust management systems have been implemented in eCommerce, as a way of assessing the trustworthiness of participants and have been credited with these trust management systems' successes [110]. Trust management can be defined as the activity of collecting, codifying, analysing and presenting relevant evidence for the purpose of making assessments and decisions regarding eCommerce transactions. eCommerce trust management is based on the assumption that one receives feedback many times and that past behaviour will be sustained. This introduces special requirements for eCommerce to embed trust management mechanisms for managing trust among various online trading partners. As trust management systems depend on feedback ratings provided by the trading partners, they are fallible to strategic manipulation of the feedback attacks. In addition, the fast development of advance computing and communication technology, introduce further challenges on the quality of trust management. As business transactions span across different countries with many organizations, a trust management system must be capable to support all different trust relationships within the domain as well as enable applications to navigate with confident. Therefore, trust management must ensure the effectiveness and efficiency of a system to increase the customer trust. It must enable users to have a prevailing degree of confidence when using the system. The ability to access the risk of entities it encounters must be given. More importantly, users can be given the assurance that the necessary security measures in place are being used effectively.

This thesis is driven by the fact that we lack an effective trust management solution for eCommerce environment.

1.2.1 Modelling Issues in Trust Management

The effectiveness of a trust management system depends on the trust model behind the system. A main requirement in eCommerce is the need of designing reliable methodology to model trust that is capable of supporting all different trust relationships. Although a variety of trust models are available to improve participants' confidence, it is still not well understood what fundamental criteria the trust models must follow.

1.2.2 Accuracy Issues in Trust Management

Another major challenge of the trust management system is to make accurate trust information in an eCommerce environment. Inaccurate of trust information have a significant impact on eCommerce participants. One of the main problems is the potential manipulations of trust by malicious players. There have already been many eCommerce trust management systems proposed in literature, but these trust management systems are susceptible to falsified ratings [6], [17], [26]. A small percentage of falsified ratings could compromise the overall trustworthiness of the participating parties as well as degrade the accuracy of the trust management systems. Several unaddressed threats still limit the effectiveness of reputation systems. Without an effective method of assessing trust, a customer's perception of risk associated with a transaction will tend to predominate a customers decision to engage in a transaction.

1.3 Research Problems

The key reason of this thesis is that we lack of an effective trust management solution for eCommerce in an open environment. In this research I will focus on enhancing the effectiveness of a trust management system thus building up trust relationship among its users. Managing trust in such an environment is crucial in improving current eCommerce deficiency. Increasing trust among buyers and sellers is thus a crucial factor that must be tackled. While designing the trust management model I will identify and investigate the following four research issues:

1. **How to unify framework and cover a broad variety of trust mechanisms?** Without providing a unified and broad framework for trust, it is very challenging to define a suitable trust management model for eCommerce. The framework should provide essential security services, such as validating the identity, providing services, securing storage, to support privacy and providing an efficient and effectively trust decision tool. Here the focus is on improving the overall architecture used in developing an ideal trust management to improve the support for existing trust management in eCommerce. Finding the requirement of a reliable trust modelling methodology is essential, and thus by applying the model to build up a trusted system. The current trust management systems lack a consistent model to help managing trust.
2. **How to reduce and manage ratings deception?** There is typically an assumption that feedback ratings are truthful and unbiased. However, this may not always be the case. Feedback data can be manipulated by malicious participants by submitting fraudulent transactions. Fraudulent sellers or buyers could also build up their positive reputations by malicious way which is an

obvious problem. Such feedback-related vulnerabilities have been identified in [23], [67]. Applying an appropriate filtering technique to the collected feedback data could help the trust management system make their transactions more smoothly and safely.

3. **How does the using of different context and factors help improve the accuracy of trust values?** - Trust evaluation techniques must accurately reflect the contributing evidence to improve the customers' confidence. Trust model must be able to maintain accuracy even under dynamic condition, adapting to changes introduced by others. Existing work on eCommerce trust systems often compute trust based on overall performance instead of individual service performance. That is the contextual relevance of evidence is not taken into account for trust evaluation. For example, a participant may have many transactions of small value items and provide either positive or negative feedback ratings to influence the trust value of either party. The trust evaluation schemes must encompass the ability to reduce this type of feedback ratings. Trust evidence requires a formal evaluation scheme to represent the relationships between different entities. This is to ensure the trust relationship established for an intended purpose and sustained until the purpose is fulfilled.

4. **How can a trust model predict risk before transaction?** According to Amland [4], information about history and knowledge of previously identified risk helps to predict risks correctly and increases customers' confidence. Thus, one way to address uncertainties is to develop strategies to determine the risk of an eCommerce transaction. Finding prediction technique that can inform potential buyers the risk level associated with a given product and develop a

system that can assists buyers in assessing the level of trust they should place on an eCommerce transaction enhance the effectiveness of trust management system.

1.4 Contributions and Significance

This thesis studies the methodologies and the mechanisms of providing a trustworthy management system for eCommerce. It seeks solutions to support trust management for eCommerce in an online trading environment. The main contributions are summarized below:

1. **Analysing the current trust management systems.** In order to produce meaningful results in trust management, it is necessary to first, understand the complexity of the area being investigated and then be able to identify and focus on the most pending of problems area. Thid study provides a comprehensive review of trust perspective, trust modelling, trust evaluation and trust management. The goal of this study is to understand and the strength and limitation of existing trust management systems. The analysis helps to identify threats of trust management systems.
2. **Developing a multilevel eCommerce trust management framework.** This framework presents a conceptual architecture with proposed desire properties that expect to improve trust assessments and decisions towards establishing a trusted eCommerce management system.
3. **Developing a suitable feedback credibility verifying scheme.** This verifying scheme aims at improving the accuracy of trust evaluation. The work introduces a verifying schemes to eliminate malicious feedback ratings received from eCommerce's' participants. This scheme benefits the trust system for finding trust issues and identifying trust evaluation problems.

4. **Developing a risk based trust evaluation scheme for eCommerce**. The design of this scheme is to help online buyers' decision making process by exposing the potential risk levels of a given transaction and allowing a buyer to make an informed decision before proceeding with the purchase of a product.

1.5 Research Methodology

System modelling and simulation methodology is carried out throughout the research work. This method examines the research work to demonstrate two important concepts: proof-of-concept and proof-of-performance.

To demonstrate the proof-of-concept, important steps were performed. Firstly, the research area within trust management is critically reviewed to provide the overview that leads to the formulation of valid problem statements. From this review, the research work is justified. Then, the proposed conceptual framework of the service-oriented multilevel architecture is designed and analytically analysed.

Proof-of-performance is demonstrated by conducting the implementation of the feedback verification scheme and trust and risk scheme using simulations. In these simulations, various parameters and workloads were used to examine and demonstrate the viability of the proposed solutions compared to similar competitive solutions. Also, analytical analysis of proposed solution is performed to evaluate its correctness.

1.6 Thesis Outline

This thesis consists of six chapters. **Chapter 1** presents a brief introduction of trust management in eCommerce. It presents an overview of some current issues and open research questions. It then present and discuss the major research contribution of this thesis and its significance. The rest of the thesis consists of several independent, but closely related chapters.

Chapter 2 provides an extensive literature review of trust management systems. It shows reliable reputation systems still remains a challenge. The chapter presents a comprehensive review of trust modelling and trust evaluation mechanism. Some of the trust and reputation challenges involve in eCommerce trust management system and how these challenges are being solved by current work are covered. The background of trust management system and previous work done on trust and trust management are presented in the literature. The discussion and understanding gained from the literature study helps our work towards solving special issues of trust and proposes new schemes in the coming chapters.

Chapter 3 helps discover the strength and limitation of existing trust management systems. The investigation is beneficial for establishing the essential elements of an eCommerce trust management system. This chapter describes some of the most important challenges and security threats that can compromise the effectiveness of eCommerce trust management systems. This chapter presents the analysis of the main challenges directly related to eCommerce trust management systems. It also presents a new multilevel trust management framework to solve trust related issues in the online eCommerce environment. This work aims to improve the support for existing trust management system in eCommerce. A case study is present to evaluate the frame work. The chapter describes several possible dimensions of an attack over trust management systems. The discussion of this chapter provides impetus for the rest of the chapters.

Chapter 4 presents a feedback credibility verifier framework for eCommerce. The new feedback credibility verifier introduces a new scheme aims to eliminate falsified and malicious feedback ratings received from eCommerce' participants. The viability of the proposed approach shows that the proposed approach can be highly effective in identifying the falsified and malicious feedback ratings.

Chapter 5 presents a new multi-attribute trust management model for managing trust among eCommerce trading parties. The formal risk based mechanism for trust management includes a number of algorithms for trust assessment. In addition, I propose a methodology for predicting the risk of selection services based on an adaptive trust control model support trust management. This is useful to online buyers as it allows them to be aware of the risk level and subsequently take the appropriate actions to minimise potential risks before engaging in a risky eCommerce transaction. Results of various simulation experiments show that the proposed multi-attribute trust management system can be highly effective in identifying risky transaction in electronic market places.

Chapter 6 summarizes the main contribution of the thesis and proposes some possible future work.

Chapter 2

Literature Review

This chapter reviews current literature in the context of the research problem detailed in Chapter 1. This chapter provides a survey and critical analysis of trust management issues and challenges associated with eCommerce. The chapter describes eCommerce and the notion of trust and trust management in eCommerce and identifies eCommerce threats and vulnerabilities and various trust management approaches to address the risks.

2.1 eCommerce

The terms ‘eCommerce’ and ‘eBusiness’ are often used interchangeably but there are differences between eBusiness and eCommerce. eBusiness covers online business functions, including all Internet based interactions with business partners, suppliers and customers such as: selling direct to consumers, manufacturers and suppliers; monitoring and exchanging information and collaborative product design [32]. eCommerce is actually a subset of eBusiness [32]. In its simplest form, eCommerce is composed of buyers, sellers, products and payment processing center.

ECommerce can be categorized into four main types: Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Business (C2B), and Consumer-to-Consumer (C2C).

B2B is the exchange of products, services, or information between businesses. A B2B company focuses on relationship building and communication using marketing activities that generate sales usually a multi-step process involving more than one person. On the other hand, C2B eCommerce occurs where a consumer requests a specific service from a business and C2C is defined as individuals doing business in an online environment. The main focus of this study, B2C is used by businesses to sell products or services to end users. It may also describe a company that provides goods or services for consumers.

2.1.1 B2C eCommerce

Business-to-Consumer (B2C) eCommerce is becoming an increasingly common part of daily life, offering consumers substantial economic and social benefits such as greater choice and convenience, increased competition and more information on the products and services they purchase. In its simplest form, B2C eCommerce is composed of buyers, sellers, products and payment processing centre. Figure 2.1 shows the basic system components of B2C eCommerce.

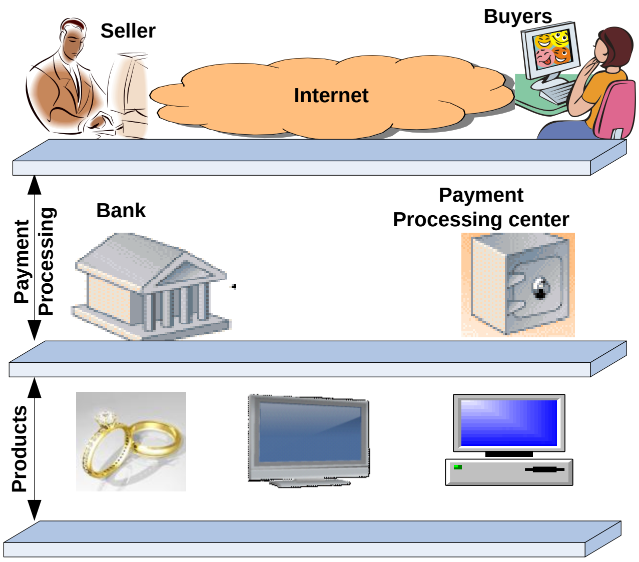


Figure 2.1: High level architecture of electronic commerce[31]

The components ordered in a three-layered of architecture: infrastructure, services, and products and structure. The infrastructure of telecommunications forms an important base for eCommerce. This includes Internet / intranet/ extranet and multimedia applications, the network technologies and transmission where it allows eCommerce activities to be fully functional. The services layer is responsible for delivers the important services for eCommerce; specifically, authentication services, Internet payment systems services and managing catalogue and directories and the security of eCommerce information. The product and structure layer allows linkages between sellers and buyers. This layer provides services for online marketing allowing remote customer to do online shopping. For example, catalogue searching and product purchase as well as provides services such as retailing, banking and other Internet commerce activities. The structure of this layer allows buyers to make payment for products purchased through Internet payment systems. B2C eCommerce is considered a necessary channel for business trading. Buyers browse the catalogue of the merchandise, choose one or more products and pay for the order. The payment processing components enable funds to be transferred electronically between the involved parties no matter where they are in the world.

These components collectively cover most, if not all, phases of eCommerce business transactions such as orders and payments, marketing and distribution. They enable sellers to advertise products and services, and deliver goods and services electronically and provide ongoing customer support. These components also enable buyers to enquire about products and services, place orders, pay for it and receive goods and services online. Sellers have web site displaying information about the products, prices, manufacturers, product warranties, etc.

The last decade has witnessed a considerable increase in the use of eCommerce by a wide range of businesses, organizations and institutions globally. eCommerce is a relatively new form of trading and it is now a major strategic move for many organizations. It has grown at a rapid pace over the last few years and has changed the way in which trading parties transact and businesses are conducted. eCommerce has the capability of providing continuous service by offering access to information around the clock and globe in multiple languages.

eCommerce has brought about a new set of opportunities and challenges to businesses, as a new business can start trading online for as little as $2000 [98]. There is an explosion of online traders in every sphere of trading. As shown in Figure 2.2, there is a steady growth in online sales and the trend is expected to grow for the next few years [94]. Online retail in the US reached $175 billion in 2007 and is projected to grow to $335 billion by 2012 [34].

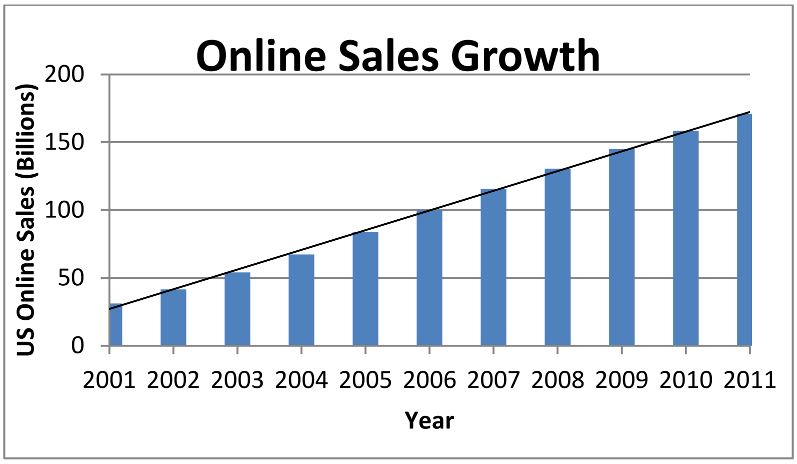


Figure 2.2: Prediction of eCommerce growth

Theoretically, both consumers and businesses stand to benefit from eCommerce regardless the types of businesses. eCommerce enables businesses to target a wider variety of consumers as well as easily and cost effectively reaches a worldwide market. By enabling businesses to expand their customer base internationally, eCommerce opens markets and potential customers that were once inaccessible to businesses. As it permits the instant establishment of virtual branches anywhere, eCommerce removes the need for physical presence at every location where the business wants to conduct sales as such saving the businesses on the lease of expensive retail space and outfit stores. Also, it allows direct and immediate overseas market entry thus eroding the competitive advantages of scale economies while improving business competitiveness locally, nationally and internationally.

The consumers gain greater choice amongst a wider and more diverse range of products and services thus making them to no longer be restricted to what are available in their local store. eCommerce gives the consumers the ability to browse and purchase from many different sellers at competitive prices and greater value, making it easier to find exactly what they are looking for. However, for the online consumer, eCommerce has many characteristics which make it different from shop-front purchases. In an in-store purchase scenario, consumers generally carry their product with them, knowing what they have purchased, the size and texture all previewed to check the contents. This is usually not possible with an eCommerce purchase where the customer must wait until delivery to ascertain exactly what they have purchased and if it meets their expectations of quality and specifications.

However, eCommerce has also opened up more opportunities for unlawful activities. The open and anonymous nature of an eCommerce makes it an ideal medium for malicious activities. As a result, eCommerce is fraught with a whole new type of fraud, deception, theft and extortion. This type of Internet marketing fraud perpetrated by dishonest Internet marketing sites involves a variety of products and services. If left unaddressed, these issues have the potential to impair consumers' confidence in eCommerce and to inhibit the growth of online markets, denying consumers and businesses the full advantages that these markets have to offer. In addition to the illicit activities, factors such as the increased uncertainty about the identity and address of the retailer, inability to inspect goods prior to purchase, the requirements to pay in advance of receipt of goods have elevated uncertainty about the performance of the product. These factors have generally reduced consumer confidence that made establishing trust between retailers and consumers difficult [17], [33]. As a result, it has hindered the uptake of electronic commerce and retarded eCommerce from reaching its full potential [17], [89]. For example, the number of online buyers globally increased only by 9.2% in 2006 compared to an average annual growth rate of 21.3% between 2002 and 2005.

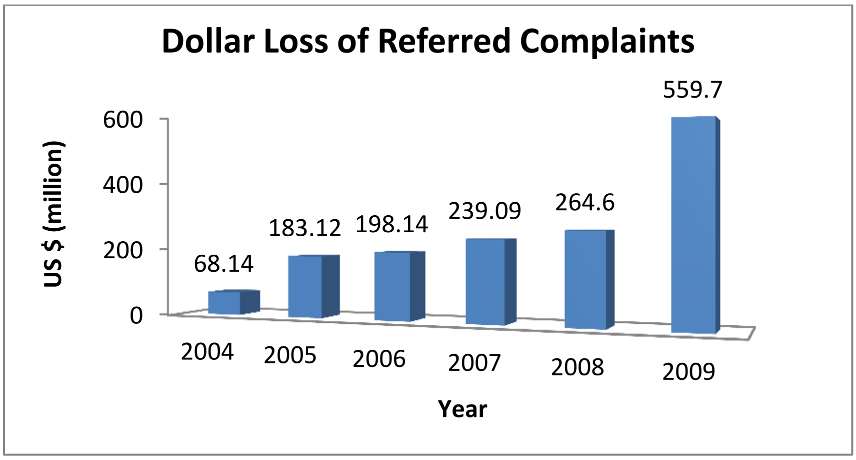


Figure 2.3: Comparison of yearly dollar loss of referred complaints

The dynamic and constantly evolving of eCommerce supported by technologies that are constantly changing increases the Internet fraud on eCommerce. Online fraud is increasing and cost online businesses millions of dollars. Figure 2.3 shows the IC3 report [46] of the dollar loss to fraud between year 2004 and year 2009. In the year 2004, the dollar loss to fraud was 68 million. In the following year, 2005 fraud on transactions went increases more than 2 and half time to 183 million. In year 2006, 2007 and 2008 show the increase of dollar loss of fraud has been relatively stable, but the dollar loss to fraud has been growing every year. By the year 2009, the total loss was nearly 560 million.

2.2 Risk in eCommerce

The increasing online fraud is but one factor for eroding online customer confidences in eCommerce. A survey report in Pew Internet shows that more people would shop online if they trusted the eCommerce environment more [71]. According to the Internet Crime watch, there is a particular concern about risks involving remote online shopping [46] due to the open and anonymous nature of eCommerce which presents potential risks to the online buyers. From the customers' prospective, risk becomes an important factor in electronic shopping [7], [8]. The risk can be the risk of monetary loss arising from online shopping due to the unreliability of vendors or about whether the purchased goods or services are able to meet customers' expectations. There is evidence that consumers consider product perceptions as more important in completing transactions [7]. The consumer's perception of risk associated with the transaction will tend to predominate in customers decision to engage in a transaction [87].

There is a high degree of uncertainty in eCommerce as buyers and sellers are geographically separated and anonymous from one another [6]. Although transaction risk is always present in all businesses and eCommerce is no exception, there are many uncertainties that could diminish potential buyers' confidence [64]. Since eCommerce enables transactions among trading parties who have never have business transaction before, it changes the business engagement rules on many aspects. Unlike the traditional store environment where payment and delivery can be effected concurrently, many purchases are delivered after payment is made. Also, the lack of face-to-face interaction between the consumers and the traders constitutes a problem for choosing a suitable trading partner. In brick-and-mortar environments, a wide range of informal mechanisms (e.g., meeting face-to-face) and formal institutions (e.g., written contracts and commercial law) have been established to reduce potential risks and thus facilitate trade between the trading partners. Moreover, consumers accept the risks of purchasing because they can see and touch the products and make judgments about the store they purchasing from. Also, often rational but sometimes purely intuitive cues such as appearance, the tone of trading partner voice or body language are used to trust or distrust potential trading partners. Without these cues, it is much more difficult to assess the safety of a business on the Internet. This suggests that perceived risk is an important ingredient in the consumer decision-making process and often translates into their reluctance to engage in online transactions.

Customers purchase online because it is convenient, without sales pressure, and saves time [42]. However, a substantial number of customers often browse items online but with no intention to buy. Statistics Canada found that 57% of Internet users like to window shop online, while a quarter less are willing to buy online [33] and up to 75 percent of online shoppers do not complete the purchases [95]. In Australia, it is estimated that almost half of Australian consumers have experience being online, only slightly more than 5% of them are willing to actually complete an online purchase [63]. These evidences clearly suggest that consumers need to feel a greater degree of trust in eCommerce if eCommerce is ever going to become a mainstream way of conducting Business-to-Consumer (B2C) transactions. It has been shown that, with respect to an eCommerce transaction, the level of trust has an approximate inverse relationship to the degree of risk [84].

2.3 Trust and Reputation

In the online eCommerce environment trust relationship between customer and supplier is especially imperative. When decision making is too complex or the stakes are too high, quite often buyers are not sure or do not know who to trust and what to decide. They rely on trustworthiness or reputation of each other.

2.3.1 Trustworthiness

Trustworthiness is the value of trust given to a person and a trust value is the measurement or quantification assigned by an entity to its belief in the trustworthiness of another entity. Trustworthiness is the opinion one has of an entity based on the history of interactions with each other [59]. Trustworthiness is modelled with a value, called trust value. A trust value represents the collective evaluation of a group of target users. That means the estimation of trustworthiness of users in that particular domain. A technical approach is used in which the factors influencing trust will be evaluated before the establishment of trust value. It is essential to identify the proper data in order for trust evaluation mechanism to obtain accurate trust value. The trust value often indicates the expectation of a successful interaction, through which some desired outcome will be achieved. A trustworthy person is someone in whom you can place our trust and rest assured that the trust will not be betrayed.

2.3.2 Reputation

Reputation is typically used to determine the degree to which can be trusted. Generally, reputation is defined as the opinion of a group of entities toward a person, a group of people, or an organization on certain criterion. For example, reputation was addressed as an assessment based on the history of trustworthiness of an entity [75]. However, Abdul-Rahman and Hailes [2] defined reputation as '*expectation about an individual behaviour based on information about or observations of its past behaviour*' and includes personal opinions as well as the opinions of others. The authors of [52] argue that reputation is a method of building trust as reputation is a collection of transactions information which is aggregated to measure the trustworthiness of an entity with regard to reliability in interaction.

Reputation can be divided into two groups: individual reputation and group of reputation. ReGret [78] is an example of group reputation. In the model, each of the entities has their reputation value, and a global reputation is evaluated based on the reputation of the entities. Whereas eBay [31] and Amazon [3] concentrate on evaluates the reputation of individuals. Individual reputation is determined in several ways. For example, a person may either rely on his direct experiences, or rely on the experiences of other people, or a combination of both to determine the reputation of another person. Opinions from direct experiences are referred to an entity that has direct interactions with a participant. Indirect experiences refer to opinions from third parties, such evidence also referred to words of mouth. A more reputed individual is generally considered to be trustworthy. Reputation is also an important factor for eCommerce and has traditionally been used as an input in decision-making process when there is lack of personal experience with an individual. Reputation has been used to model the trustworthiness of eCommerce's online participants [107].

2.3.3 Definition of Trust

Trust is described as the assurance for a long-term relationship between business trading partners [8]. Also, trust is essential to risky situations [87] or as a risk management approach where future interactions are difficult to predict [34]. Consumers make buying decisions based on trust and other factors such as security, comfort and quality [71]. Trust is a fundamental element for interactions between humans and organizations in every day decision-making process. Trust has been recognized as a complicated concept. While there are many definitions of trust from a broad range of disciplines, there is no one commonly shared understanding of what trust actually means [41]. Trust is a multidimensional concept that has been studied from the viewpoint of many disciplines, including sociology, social psychology, and economics [10], [22], [84].

Sociologists view trust as the foundation of the social order and is the basic standard of social contact. According to Gambetta [35] trust refers to the subjective probability an individual expects another individual to performs a given action on which its welfare depends. Nancy Carter and J. Mark Weber [70] found that some assume that people are generally untrustworthy and act accordingly until their counterparts show their trustworthiness gradually over time. They also stated that others assume that people are generally trustworthy, but make themselves vulnerable to their counterparts until evidence challenges their trustworthiness assumptions.

Psychologists tend to focus on trust as a person's attitude and a person's mind rather than an intellectual thing. It is believed that trust is integral to the idea of social influenced and trust is a psychological state in which people make a decision based on their attitude and mind. One popular definition about trust given by Morton Deutch is that the construction of trust is very much time related in nature and trust increases willingness of people to accept vulnerability [26]. Psychological relationships have been largely conceptualized in the literature as the degree to which an individual belief obligations, because perceived or real promises has been made. Moreover, psychologists studied this topic trying to distinguish the several mental situations similar to trust. For example, trust in someone's status or trust in a brand name of a product. Trust as risk-taking, an individual would be prepared to take that risk in an uncertainty situation.

Economists usually quantify trust in monetary terms. Economists believe trust help reduce the cost of transactions. They believe that trust enable cooperation between buyers and sellers and generally furthering business activities. They analyze trust from the perspective of utility (cost and benefit).

Probability theory [50], [53] and Game theory [110] are the most popular tools used by computer scientists to study how entities develop their trust relationship in uncertainty environment. Probability theory is based on human's psychological state, and uses a range of mathematical function to differentiate the honest and dishonest participant within a relationship. In game theory, strategies, such as tit for tat, cooperation or defection are used. The Prisoner's Dilemma is an often used to link trust and with economic utility. Several characteristics of trust observed from all different disciplines include the following:

1. **Subjective Degree of Belief-** Subjective degree of belief means one party believes that another party can perform an action in a certain situation. For example, given a book review from Amazon website, different people may have different opinions about its quality as it mainly depends on the taste of each individual. Falcone and Castelfranchi [15] recognise this trust as reliability. They also advised that have high reliability trust in a person is not necessarily enough to decide to enter into a situation of dependence with that person. The work of [52] further identified this definition of trust as reliability trust and decision trust. They suggest that reliability trust includes the concept of dependence on a trusted party and the reliability of the trusted party by a trusting party.
2. **Context Dependent -** Trust is context dependable. Context is a set of attributes or facts that surround a particular situation. This may include variation in role, time and other environment factors, but it may additionally include others specific information that can be used to characterise the situation involving entities. For instance, an organisation involved in many different trust relationships with many customers and a number of suppliers of goods and services. A service provider may be dependent on other sellers which has its own trust relationships. For example, seller S1 trusts seller S2 on its quality of the service but not on its delivery time. Whereas, S3 trusts seller S2 on its deliver service not the quality of service. Any changes of a dependable

contextual may affect the degree of trust of entities. As such the customer may have different trust relationships with all different sellers within that specific context. In addition, these trust relationship for a given context in a given time may be evaluated differently at a later stage. A trust relationship between both customers and sellers may also gradually degrade if there is no transaction takes place between them [51]. This means that trust relationship of entities is time dependant, and it is necessary to take time into account when evaluating of trustworthiness of entities.

3. **Objective Properties -** Trust is objective properties when the trust level of an entity is measurable. Trust is measurable such as the policy or warranty specified by entities for a trust decision. An entity's trustworthiness is quite often related to the quality of its services provides to others. If the quality of a service can be objectively measured, then that service is called objective trust. For example, a website provides information about warranty policy of an organisation and this information can be checked against the official data released by that organisation. It is different from subjective degree of belief that trust is relying on the opinion of others and it cannot be objectively measured.
4. **Assessable -** Trust is assessable as it provides the foundation for trust modelling and computational evaluation. Trust functions have a direct impact on one's decision regarding information collection and other critical tasks. And that trust values can be used to represent the different degrees of trust an entity may have in another.

5. **Dynamic -** Trust relationship between entities is dynamic. Trust can be change with further interactions. Trust relationship can be either continuously growing or developing within group or it can decay over with time. Thus, trust is dynamically time-sensitive and trust mechanism must responses to rapidly changing conditions under specific circumstances. It must be able to support of dynamically changing of such trust relationship and the updated trust information is made available for users.

Trust assessment for eCommerce must be based on all the evidence that can be practically collected and should provide a basis for decision-making. These collective factors discussed earlier, create interactive elements are the important guidelines for trust modelling in eCommerce trust management system. All these important factors are important features for making trust evaluation. From the above discussion, the assessment of trust in eCommerce is based on a number of referents that construct confidence between eCommerce participants, such as reliability, availability, dependability, and competence.

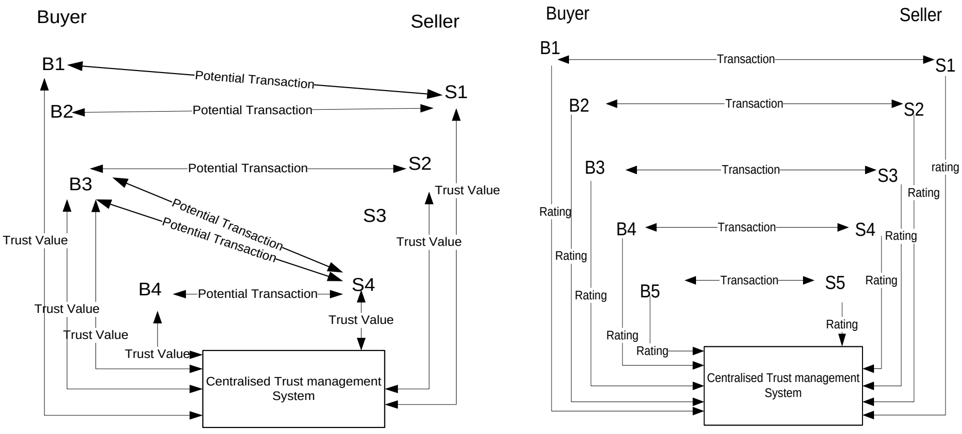
2.4 Trust Management System

Trust management systems are emerging as a promising technology to improve the eCommerce customer and supplier relationship. As define in Blaze [7] trust management involves three processes*:* collection of information, evaluation of trust relationship and disseminate relevant trust evidence that help decision making regarding eCommerce transactions.

A specific method uses to process and control trust relationships among participants is referred to as a trust model. A trust model is a simplification of the complexity of trust and it is an important risk management mechanism in such online communities. However, participants of online trading are still sceptical of the existing trust models due to lack of a specific criterion for the design and implementing a feasible and efficient eCommerce trust model. With the rapid development of network and communication technologies, designing updates of eCommerce trust models is essential to improve the effectiveness and management efficiency of a eCommerce trust management system. The challenge lies in finding ways to gather relevant evidence and methods for trust assessments in the eCommerce environment. To find the right methods, we must first have an understanding of the network architecture of trust management systems (TMS).

2.4.1 Network Architecture

It is important to understand the network architecture of a trust management system, as it determines the method of collecting feedback ratings and propagation of trust value between participants in the community. There are two commonly used network architectures in developing a trust management system: centralised and distributed architecture. Figure 2.4 and Figure 2.5 show the differences between the centralised and distributed network architecture in a rating trust management system. In a *centralised model*, there is a central entity takes all the responsibilities of managing trust for all participants. Typically, trust information of the registered participants is gathered and evaluated constantly and updated information is made available to the public. The trust values are computed in many ways and are updated as a function of the received ratings. Participants can then use these trust values to decide whether to transact with a particular participant according to their own risk perception. Figure 2.4 (a) and (b) show a common type of centralised trust model.



(a) (b)

Figure 2.4 Generic centralised trust management network architecture

In this model buyers and sellers provide feedback ratings about their performance of each of the transaction they had participated. These ratings are collected and assesses by the trust management system, and trust value of each participant is updated constantly. Comparing with distributed system, the centralised system is less complex and is easier to implement. However, eCommerce trust system have enormous amount of transaction information, computing and storage of such information is often an issue that effects the accuracy of trust information. For example, eBay is an open centralised system that gathers customer profile. Its data is then stored and managed by a centralized database system. Information about the performance of a given participant is collected and these trust information is publicly available to its registered users.

eBay[31] is one of the popular centralised reputation-based system uses such method to evaluate participants' reputation score. The other simple method used by Amazon is average feedback ratings. As the simple summation method is used to evaluate reputation information of users, it created challenges for both buyers and sellers. The accuracy of the reputation or trust value of entities is questionable. Moreover, participants can easily misbehave in buying and selling in eCommerce environment. In this centralised system, authorization is based on the assumption that all of the participants are known and their identity can be established using an authentication system. Reputation system enforces security policies and rules between both the provider and consumers against security fraud but this policy does not authenticate individual participant. Thus, such systems have no information about the identity of reviewers. Malicious participants can manipulate feedback data by submitting fraudulent transactions. Fraudulent sellers or buyers could also build up their positive reputations via malicious methods. For example, users selling numerous low priced items and have positive behaviour to increase the number of their feedback ratings and then engaging in fraud with higher price items. The majority of feedback received by eBay were almost always positive [75], [76]. This indicates that the participants are not telling the truth due to worry of revenge feedback. Buyer can register as a seller at the same time using different identity to provide feedback as it is easy to change someone's identity in online communities [27], [59]. Buyers/sellers may risk in participating in a transaction with untrustworthy buyers/sellers. After cheating thus resulting a bad trust value or reputation, a fraudulent sellers or buyers can discard a current identity, register and establish a new identity then continue to trade and start to build a new reputation. A variety of techniques have been proposed to protect the identity of an individual. Some more sophisticated techniques advocate the use of pseudonyms to protect privacy [40], [68]. However, Bradley, the author of [65] declare that the claim of pseudonyms protect privacy is fundamentally flawed for a variety of reasons. The challenges of this system has been study and identified by many researchers. The following are some of the common drawback identified by researchers [24], [51], [75] and are summarised as follows:

1. Simple summation method is scalable and easy to implement, but lack in flexibility. The volume of everyday incoming data causes slow response times to counteract new threats to the system.
2. Inaccurate trust results. The system used unreliable feedback ratings to compute the reputation or trust-level of an entity. Unreliable feedback rating is one of the reasons that affect the accuracy of results.
3. Another problem of the system is the difficulty of obtaining feedback ratings. Many participants do not bother to provide feedback ratings after completing a

transaction. The issue of difficulties in eliciting feedback has been discussed by both works done by authors of [24] and [51].

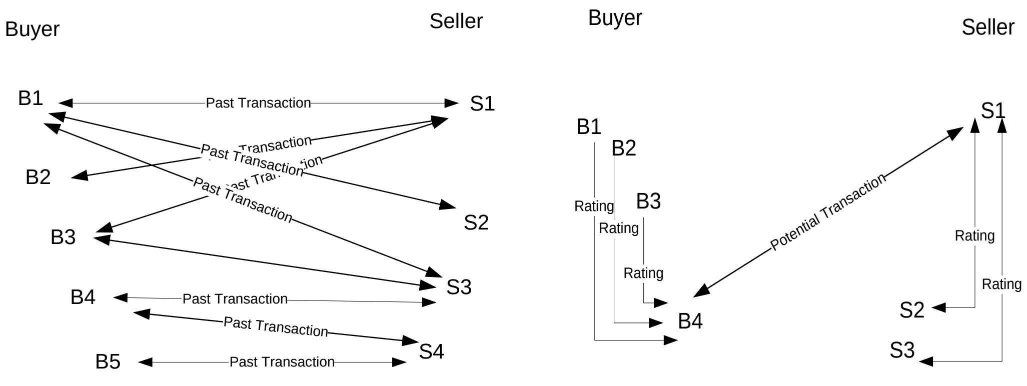
4. Simple summation evaluation method is especially difficult to represent the actual trustworthiness of a participant when there is a negative outcome.

Amazon [3] is another eCommerce site on a B2C eBusiness model with centralised network architecture. It is an online store that allows members to write review of its products and it allows anybody to sign up as a member. Unlike eBay only allowing a feedback rating after a completed transaction, Amazon encourages registered participants to provide ratings regardless whether they have any transactions with them. The review rating is in the range 1 to 5 stars. The trust reputation measure of a product or service is calculated as an average of all the recommendation ratings received. It displays evaluation results for participants in order to offer other participants regarding reliable products or services on the sites in order to maintain their competitiveness. Users may use the evaluation result to determine which sellers to buy from.

1. Amazon does not pay reviewers to review products and services. However, this does not mean suppliers or the book writers and publishes are doing the same. Financial incentive can influence the ratings given by reviewers. Those recommendation ratings, however may not honest and reliable.
2. Malicious reviewers may give misleading recommendation ratings for personal gains. For example: a reviewer may give bad ratings to all competitors; malicious reviewers may collude to give good ratings or bad ratings to a provider depending to the reasons.

3. On the other hand, personal experiences may differ. This system faces the similar problem as eBay. Recommendation ratings from reviewers may not reliable, thus the evaluation result may not be accurate.

In contrast, *distributed system* gives individuals the responsibility to control over their own resources with little or no consideration of others. Figure 2.5(a) and 2.5(b) illustrated how ratings are collected and stored in a distributed model. There is no common place for participants to share their experiences, thus the method of feedback collection and evaluation service is up to the individual participant.



(a) (b)

Figure 2.5 Generic distributed trust management network architecture

Each of the participants keeps their trust information to themselves and compute their past experience with others or they may be a distributed store where ratings can be submitted and evaluated. This trust information may be available to participants when requested. This does not mean all trust information is accessible everywhere to everyone. Any party, who considers a business transaction with a particular party, must either get trust information of this particular party from the distributed store or get information from others who have had past experience and are willing to participate. The evaluation function can be based on feedback ratings from own personal experiences or from other’s experience or a combination of both. Normally, the own experiences are considered more reliable than those from the third parties and therefore weighing heavier then the others.

2.4.2 Trust Management Systems Challenges

The goal of the trust management systems is to manage the trust relationships between business partners. This goal is achieved by maintaining the trust-level of the eCommerce participants and makes them available to potential eCommerce customers when needed. The trust level is derived from feedback ratings submitted by the trading partners after the successful completion of the transactions. The submitted feedbacks are analysed, aggregated, and made publicly available to the interested parties.

The eCommerce environment must be able to ensure the accuracy of trust value by any means and puts forth a strong trust management mechanism in place. Without proper trust management mechanisms, the involved parties, either a buyer or a seller, may invoke fraudulent activities, thereby causing loss to the other. A trust management system must be able to help participants locate trustworthy partners and do business transaction securely with confidence. The effectiveness of a reputation trust management system depends on the trust model behind the system. eCommerce trust management systems still encounter considerable challenges and are incapable of supporting all different trust relationships to improve participants’ confidence. There are many relevant factors that influence potential buyers to make decisions.

One of the main reasons is the potential manipulations of trust by malicious players. Inaccurate trust information has a significant impact on eCommerce participants. Thus, the major challenge of the trust management system is ensuring the accuracy of trust information. When developing and designing a trust management system, the most important procedure is to recognize and understand the type of security threats to the trust information. There is also a need to consider what types of countermeasure should be implemented to prevent such threats. In order to improve a trust management system effectively and efficiently, the potential threats must be identified and actioning to prevent any damage.

A security threat is the type of threat that is likely to cause damage of trust information accuracy, whereas a vulnerability is the level of exposure to threats in a particular context. Security threats are the main concern of designing and developing an efficient trust management system. An imprecise management of these threats could result of security deficiencies and weakness of a trust management system. However, not all trust models address know all possible threats that undermine the accuracy of trust management system. Identifying these security threats helps the trust management system in improve vulnerability measures thus reducing or removing known weaknesses in the eCommerce environment. The open nature of eCommerce trust management systems, both either centralised or decentralised architecture, are susceptible to the following critical threats and attacks due to the presence of malicious participants. If a trust management system is compromised under a malicious attack, it can start giving out false trust information to a request, such as returning false data to a search query. Following is the description of some of the attacks common on eCommerce trust management systems.

1. **Denial of Service -** In an open architecture, malicious participants may launch an attack on individuals or groups of participants to disable the service. One of the attacks is denial of service (DoS). The primary goal of denial of service attacks is to disable the system or make it impossible for normal operation to occur. These attacks can be easily initiated if a centralised trust management system is deployed. The most common and obvious types of DoS attacks occurs when an attacker "floods" a network with information. Such kind of attacks are caused by malicious individuals continually issuing messages which overloads the system network, eventually rendering the system unreliable or useless. In a DoS attack, an attacker attempts to prevent legitimate participants from accessing information or services. By targeting your computer and its network connect, or the computer and the network sites you are trying to use. An attacker may be able to prevent you from access to the trust information. Without any trust information present, there may not be enough knowledge to form relationships between both participants. Unfortunately, there are no effective ways to prevent a Dos attack, but there are steps that can take to reduce the likelihood of attacks. In order to compensate, the system requires the ability to contain the effects of denial of service attacks.

2. **Interfering of Trust Value -** Inaccurate of trust value can be due to tampering stored of trust data. Internet applications, such as eCommerce, use databases to store participants' trust values, updating them regularly to reflect the current trustworthiness of participants in the system. For eCommerce trust management system, maintaining such data is a complicated task as

participants are able to join or leave the trust system freely. One way for malicious participants to deceit the trust value is by infected the system. This can be introducing viruses, worms, Trojans and spyware to the system. Infection is usually the first step in a process aimed at stealing confidential data or opening holes in security defences for hackers to exploit. Man-in-the-middle is another security threat in which a malicious individual gets between the receiving participant and the sending participant in a network and sniffs the information being sent. Usually, this attack does not change the value of the trust information, but it allows this value being known by the public. However, the deletion or modification of the data exchange can also succeed when the attacker impersonates other party by inserting himself between two communicating parties, and both parties believe they are talking to each other.

3. **Inaccurate Trust Value.** A trust evaluation mechanism aggregates all the received information of certain participant in the community and computes a score, which result in the trust value of a participant in the network. A participant selects the most trustworthy business partner in the community providing a certain service and effectively having an interaction with it. However, this trust value may be calculated wrongly and there are a number of reasons for this possible threat. For instance, inappropriate trust metric or incomplete information is used in represents a level of trust. Another reason of inaccurate trust values is because trust evaluation is based on the contaminated feedback ratings in which these feedback being maliciously provided. In both cases, trust system must be able to verify the reliability of the trust value. The existing work on eCommerce trust system often compute trust based on overall

performance instead of individual service performance. That is the contextual relevance of evidence is not taken into account for trust evaluation. Trust evidence requires a formal evaluation scheme to represent the relationships between entities. Thus, trust evaluation schemes must accurately reflect the contributing evidence. This is to ensure the trust relationship is established for an intended purpose and is sustained until the purpose is fulfilled. The correctness of trust value is critical for eCommerce participants in decision-making. Inaccurate trust information may lead to monetary losses as participants rely on this trust information and decide to trust and transact with unreliable business partners.

4. **Unreliable Feedback -** While feedback-based rating systems are increasingly used in eCommerce environments, they are susceptible to falsified ratings. A small percentage of falsified ratings could compromise the overall trustworthiness of the participating parties as well as degrade the accuracy of the trust management system. While it is impossible to expect all reviewing participants to provide actual ratings in an open environment such as eCommerce, it is necessary to have an approach that capable of detecting falsified ratings to protect the integrity of the trust management system. Although there have been techniques to encourage trustworthy behaviour [6], [17], [26], the general trend in feedback-based trust management systems are to accept all ratings provided by the transacting partners as accurate feedback. Therefore, identifying and actioning falsified ratings remain an important and challenging task [17]. One of the major problems of existing trust management systems emanate from the unreliable feedback data used to compute the

reputation or trust-level of an entity. Given that eCommerce have serious vulnerabilities due to potential manipulations by dishonest or malicious players, it is very important to ensure that trust values of entities are accurate and not manipulated by malicious and dishonest participants. Unreliable feedback ratings are often introduced by the malicious participants. The general behavior of malicious participants has been described and the characteristics and strategies of a malicious participant are also discussed in many work. For example, Josang and Golbeck [53] discussed the various rating attack types against the trust management systems. Kerr and Cohen [57], [58] identified a number of vulnerabilities in reputation trust management: reputation Lag, value imbalance, re-entry, initial window and exist. Their recent paper [57] analyses of a set of proposed trust management system base on the identified issues. Similarly, Dellarocas [23] discussed four types of rating attacks referred to as ballot stuffing, bad-mouthing, negative discrimination and positive discrimination. Similar work proposed by [96] use explicit trust ratings and extracted trust scores from the feedback ratings to predict and prevent undesirable transactions. Yu and Singh [105] proposed a multi-agent system based on social relationship of the network, where agents represent different people. Agents interact and communicate, model and develop trust in each other. O'Donovan [28] focuses on using explicit trust expressions in social networks as a source of information.

Buyers who tend to falsify ratings have similar characteristics to online auction shilling bidders [91], [92] and [93]. Research shows that a malicious bidder in an auction site tends to have a higher bidding frequency to outbid legitimate buyers [91]. Similarly, a participant who intends to inflate or deflate a seller's reputation will attempt to submit a higher frequency of ratings so that the number of falsified ratings may outweigh the number of accurate ratings during a particular time interval. Another common characteristic is that participants who falsify ratings usually have low trust value [20], [74], [91] and [102]. They also tend to usually engage in minimum value transactions to meet the requirements of submitting a rating [91]. The following describes some possible threats to unreliable feedback.

Impersonation - It is to use another person's identity (obtained through malicious acts) to do online activity. For example, a merchant who has low trust value may impersonate someone else to give himself positive feedback ratings in order to build up his online reputation. Another possibility is to take advantage of on the pre-existing trust relationships of the identities they are impersonating, such as engages a transaction whereby it is not possible for him due to the poor reputation. As a result, either negative or positive feedback ratings may be given to the participants depending on the outcome of both parties' negotiation. Therefore, a trust system must have the ability to detect such deception.

Fraud - With no face-to-face interaction, fraud is another threat that often happens in the online communities. A fraudulent party may not completely fulfil the requirement for transactions in a system, or the availability of services that they promise does not really exist. For example, a service provider can indicate that they have a particular service available even when they knowingly do not have the offered service. A malicious participant may also falsely claim that they have delivered certain products to a peer but the peer has received no such goods. It is also possible for malicious participants to act in bad faith without actively misrepresenting themselves or their relationships with others. Feedback ratings from each other may not reflect the true of the transactions. Therefore, the system should attempt to minimize the effects of bad faith.

Misrepresentation - This happens in both tradition and electronic commerce, when participants provide misleading information about their trust relationships with other participants. Reputation or trust value of an individual is important for a business to continue their online business successfully. However, reputations of an individual can be disseminated by words of mouth or through rumours. A malicious peer may give a false value to a victim peer and communicate these incorrect values to other participants. For example, a malicious peer could actually trust a victim peer but send out reports contrary to its knowledge. These malicious groups of participants try to confuse other participants by giving either positive or negative feedback that is not the true relationship they have with this peer. Such dishonest rating strategies may be initiated by a competitor to sabotage another party. This deception could either intentionally inflate or deflate the malicious participant’s trust relationships with others. Both possibilities must be taken into consideration.

Collusion - This refers to a threat posed when a group of malicious participants collaborating and trying to sabotage the trust system to increase their own trust value or to lower the opponents’ trust value by manipulating their feedbacks. In order to benefit their group they provide positive feedback and sabotage another party by giving biased feedback. Therefore, a certain level of resistance needs to be in place to limit the effect of malicious collectives.

2.4.3 Type of Trust Management Systems

Various trust management proposals applying wide range of different mechanisms and techniques have been developed to mitigate challenges for eCommerce environments. Probability theory, collaborative filtering, policy-based and reputation-based are few types of trust management used to manage eCommerce trust relationships. Although not considered a mechanism, collaborative filtering is used to detect and get rid of biased feedback ratings. These mechanisms are supposed to support assessment of trust and the development of trust. And they also supposed to reflect trust relationships of eCommerce participants. Unfortunately, despite the growing interest in development of quality eCommerce trust management system, challenges for eCommerce trust management system remains.

2.4.3.1 Collaborative Filtering

Collaborative Filtering (CF), first introduced by Goldberg et al [37], is a technique for detecting patterns among the opinions of different users by collecting large sets of data from prior participants' information. CF is an algorithm that filters information for a user based on the collection of user profiles and make predictions about the preferences of other users. CF uses the known preferences of a group of users to make recommendations of the unknown preferences for other users of the system. The assumption is that users who have had similar preferences in the past will have similar preferences in the future. Since the collective opinion in a community determines an entity's reputation score, many Collaborative Filtering methods have been proposed and used in reputation systems. Low score or high score represents a collaborative opinion of an object that having or providing low quality or high quality respectively.

Basically, this technique relies on ratings from participants to predict and offer advice based on someone's personal preferences for information and/or products as purchases. The CF monitoring the participants' taste of product or information and then connecting that information with a database of other peoples' preferences to look for matches and is based on the assumption that similar items will interest similar consumers, with tastes in common. The assumption is that finding similar users to a new one and examining their usage patterns leads to useful recommendations for the new user.

2.4.3.2 The Probability Theory

Probability theory is based on mathematical functions that quantify uncertainty regarding the occurrence of events. It is a mathematical approach which based on application of statistical data analysis or past information to produces patterns of events that can be anticipated together with ways to represent uncertainty. Probability theory has been used in many disciplines including computer science. Probability theories are one of the most popular techniques used in reputation trust management systems to evaluate trust of entities. Probability theory usually modelling events that requiring statistical forecast. Statistical concepts solve problems in a range of contexts and are currently used in various fields such as in business and science. Statistics is the knowledge of decision making under uncertainty, which must be based on facts or some numerical and measurable scales.

In trust management system, statistical data analysis is usually based on the history of entities or their trustworthiness not on personal opinion, recommendation, nor on someone's belief. Some Bayesian approaches consider probability theory as an extension of artificial intelligence to handle uncertainty. Bayesian probability theory has been extensively studied in literature. There are many proposals used in trust management such as [11], [53], [54], [55] and [99] applied Bayesian probability theory to evaluate trust in which trust value is calculated based on the statistical updating of beta probability density functions.

2.4.4 Reputation-based Trust Management

The reputation-based trust management systems are most widely used mechanisms in eCommerce to help minimised the risk of online trading participants [14], [100]. The basic idea behind the reputation-based system is that trading partners rate each other after the conclusion of the transaction and the system aggregates the ratings and makes them available to interested users. It is also intended to make the service providers to be trustworthy to keep their customer base and attract new once.

Reputation-based trust management evaluates reputation for trustworthiness of a participant. There are three characteristics of a reputation based trust management [56] and [76]: 1) The participants have to be long lived to influence future reputation scores; 2) Mechanisms used to capture the current scores to influence future scores; 3) rating about past interactions to guide current interaction.

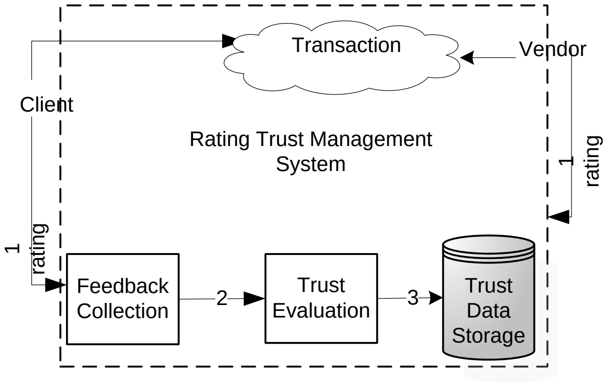


Figure 2.6: A Generic reputation eCommerce trust system

Figure 2.6 shows a rating based (reputation) trust management system. The system has the following three components:

1. **Feedback collection** refers to the collection of feedback ratings from both buyers and sellers after completed online transactions.
2. **Trust evaluation.** The aim of evaluation is to compute a trust value from the aggregation of feedback ratings. For example, eBay uses a simple summation method to compute trust value of participants.
3. **Trust data storage**. Storage is needed for maintaining past behaviours and all trust information. Mechanism may be implemented to ensure data integrity confidentiality and availability.

The basic idea behind the reputation-based system is that trading partners rate each other after the conclusion of the transaction and the system aggregates the feedback ratings and makes them available to interested users. In a distributed environment, each participant can act both as a provider and consumer of resources. Each of them is responsible for collecting and combining ratings from other participants usually from the relying neighbourhood [52]. Accordingly, how these histories are combined is varies, different system used different mechanism. Therefore, in eCommerce, the consumer is an important “information source” and the evaluation of feedback ratings received from both buyers and sellers are used as the quality indicator. In other words, both buyers and sellers play an important role as feedback rating suppliers.

2.5 Trust Evaluation Mechanisms

A trust evaluation mechanism is a component usually embedded into a trust management system for measuring levels of trust. In all reputation trust management systems the calculation of service scores is handled by the trust evaluation mechanisms. An effective trust evaluation function improves the accuracy of trust information minimises the risks associated with eCommerce. Please note the terms of “reputation”, “trustworthiness”, “trust value” and “trust level” are used to mean a trust evaluation score. It has been shown that trust associates with eCommerce can be measures according to own subjective degree of belief. The evidence is assessed accordingly to the context of the trust purpose [101]. There are a number of recent research efforts to improve eCommerce trust management systems by proposed different algorithms in trust evaluation. Some trust algorithms is built up by own experiences of the past interaction with an entity, others proposed approaches when evaluate trust value of an entity combining direct experience and recommendation from other third parties.

2.5.1 Collaborative Filtering Approach

Dellarocas [23] proposed an unfair rating filtering method by examining the ratings that are further away from the majority of ratings. These are identified as abnormal and subsequently removed. This approach is correct as long as the majority of ratings are not from a group of participants that tend to falsify their ratings. Another approach that uses beta probability density functions to estimate the reputation of seller as either bad or good is discussed in [50]. This approach was later extended such that a rate is considered to be fair if it falls in the range of lower and upper boundaries among all the ratings [99]. The limitation of this strategy is that participants could collude as a group to manipulate the majority ratings.

The works done by both [52], [107] are some of the examples using CF method to improve reputation trust management systems. Other works using this technology was proposed by Breese [9] to suggest or recommend items to user that the system think users might like. The basic idea is that all users provide their ratings of what they like or preferred. All ratings received are store for later use in a centralised storage and user profiles are keep maintains by the centralised system. User profile similarity is used as a criterion for finding possible recommendation, which is at the basis for locating expertise within a community. To predict and suggest an item to a user, the Pearson correlation method is normally used to measure the similarity between users. This similarity-based filtering technique is also used in reputation trust management system. Amazon.com [3] is one of the popular site used CF technique to make prediction and recommendation. The difference between these systems is that reputation trust system measures the trustworthiness or reputation of users, such as the work of [28], [45] and [59] used this method to filter out low similarity ratings that are seen as less trustworthy.

Zuo et al. [111] proposed an adaptive Collaborative Filtering algorithm for to avoid the bad influences of dishonest ratings. This approach based on the user profile similarity or neighbour to a given user and weighing scales to filter suspicious ratings which are from colluders or badmouthers. Algorithm used to select reliable participants of a specified target are based on direct experience and others neighbour opinions. The algorithm first evaluates a participant's own experience with the target participant, and the neighbourhood ratings separately, then both of the results are compared. The statistical difference between a participant and the neighbour ratings are calculated. This algorithm compute the ratings in which the difference is significant as the participant is identified as dishonest. Otherwise ratings are considered reliable and weighing scales are used to weight the given rating and combine them as final result. The weighing methods are applied to the ratings that are identified as dishonest. The weighing methods weight both positive ratings and negative ratings. If a participant has given several false positive ratings, he is identified as colluder. If several false negative rating has been given then he is a badmouther. The trust decision is made from a weighted summation of the ratings towards the target participant.

1. The basic process behind Collaborative Filtering requires large data sets in order to be reliable since average item and user ratings are important. Thus, one of the issues of this system is to make recommendation or prediction for new users as they have no prior information or information is sparse in this system.
2. The second problem with this approach is the possibility that unreliable reviews may be given by some of the participants. Buyers can submit ratings with the same value as many as possible to vendors. Thus, this method is inadequate to measure the trust value of users as ratings could be easily manipulated by malicious users.

3. Another disadvantage of this type of reputation evaluation mechanism is that it needs frequent involvement of users that provide ratings. Insufficient number of users is an issue of poor performance with collaborative filtering method.
4. Weighing scales used in Zuo's [111] approach to identified malicious participants may be useful if other factors such as time are taking into account. Malicious participants may used many different identities and collude to provide ratings.

2.5.2 Beta Reputation System

The authors of [50], [53] have developed a binomial Bayesian reputation systems for electronic markets. This system supports binomial which allows feedback ratings to be expressed with two values as with positive (e.g. good) or negative (e.g. bad). This system is based on distribution by modelling reputation as posterior probability using statistical estimation of a beta probability density functions to combine feedback ratings and evaluate reputation scores. Beta Reputation systems collect ratings about users or a service in a centralized evidence repository for all members of community, giving an objective measure. Its trust evaluation mechanism is employed in Bayesian reputation models and the certainty of the trust calculation is defined by mapping the beta distribution to an opinion, which describes beliefs about the truth of statements. This work implies that a trust model should be: a) able to combining feedback from different providers, b) discounting feedback in which more weight is giving to the feedback from higher reputation provider than the lower reputation providers, c) forgetting method. Less weight is given to old feedback ratings than to recent feedback ratings.

1. The advantages of the beta reputation system are flexibility and simplicity. It provides a statistically sound basis for evaluating trust measures, as well as its foundation on the theory of statistics. This system only requires two parameters for continuous updating as new observations are made or reported.
2. The disadvantage of a binomial model is that it only able to express with two values, that is positive or negative. Although it is able to expresses binary ratings with graded values by splitting the value to partially positive or partially negative, it is not flexible enough to includes ratings other than the binary value.
3. Two parameters of discounting and forgetting (aging technique) of feedback ratings are taking into account when evaluating and updating reputation score. The discounting and forgetting of feedback ratings are based on the provider's reputation and the longevity of feedback ratings. This suggests that feedback providers with higher reputation are always more reliable than those with lower reputation. Generally, this is might be the case. Forgetting and longevity of feedback ratings are important in measuring trust, but in electronics markets, these two factors are not sufficient to determine the trustworthiness of a provider. Others factors such as credibility of feedback ratings, quality of services and goods must be considered. Economic theory indicates that whatever the cause of the quality of goods and services will necessarily lead to the variation of reputation [86].

Whitby et al. [99] later extend [50]'s work proposed an approach, Travos to filter the unfair rating from the participants. This model makes use of the beta distribution to estimate the probability of honesty of a potential partner. Direct experiences are first use to evaluate a potential partner; the probability function is then used to estimate the confidence of the result of the evaluation. This work too used both factors of forgetting and longevity factors to weight feedback ratings.

It differs from Josong and Ismail's work [50] in that the filtering algorithm includes majority ratings as another factor to handle the unfair ratings among the participants. In this approach To filter the unfair ratings for a seller, all feedback ratings provided for a seller is collected and are accumulated, and the feedback ratings provided by each participant is represented by a beta distribution. When the accumulated feedback ratings (the reputation) of the seller fall between the lower bound and upper bound of these feedback ratings, it is considered as fair ratings, otherwise there are unfair ratings. However, these ratings are again as unfair high ratings and unfair low ratings by measure the location of these ratings, if there are outside the boundaries or within the black areas (accepted area). Participants rely on their own experience if the confidence level is high, otherwise, seek results from other participants, and their results are discounted based on the accuracy of prediction. The combination of both result are then combine as final trust result. The similar majority technique was proposed by Dellarocas [24] earlier to filter unfair rating by examining the ratings that are further away from the majority of ratings. These are identified as abnormal and subsequently removed.

1. Similar to [110], credibility of feedback ratings is the main issue of this approach. The filtering algorithm of this approach taking into account of majority ratings in evaluation process. This approach is accurate as long as the

majority of ratings are not from a group of participants that tend to falsify their ratings.

2. This approach uses the assumption that behaviours of rating providers remain consistent. There are dishonest users that always provide unfair ratings. Otherwise this approach could not work accordingly.
3. Another problem of this filtering approach is that all participants are assumed to be trustworthy and ratings provided are all truthful. However, this is not possible as fraudsters carry out fraudulent activities in online environment. Many works have been done on the feedback ratings credibility issues, such as [101], [111].
4. Majority rule is a binary decision rule where a positive decision is weighted more than a negative one. Nevertheless, majority rule is most often used in organisations for important decision-making. When majority of participants agreed with a same value of a feedback rating, then this ratings value should consider as truth value. In the online environment, this majority rule is only effective if majority of the ratings are from reliable participants who provide honest feedback ratings.

Yu and Singh [103], [105] proposed a distributed trust model to locate the correct witnesses in order to evaluate the trustworthiness of a service provider that is willing to participate. The evaluation process of this model is applied the Dempster Shafer Theory of Evidence approach. The proposed model is a multi-agent system in which the agents are expected to cooperate by giving, pursuing, and evaluating feedback received. The trust measure is calculated by combining an entity’s own experience and other entities’ previous experiences. Each entity has a set of friends, a subset of which are identified as its neighbours, and that an entity would refer to in order to investigate the ratings of another entity. These third parties are expected to behave responsibly and honourably. The basic idea of this model is that after a few transactions unfair ratings provided by participants who have low trust value will carry low weight and therefore will not have much influence in reputation assessment. The model assumes that all buyers in the system have provided rating for a given period of time. For example, new users who trust everyone because the new user has no experience will depend on others opinions, and the system will rate him/her as a bad user, and therefore his/her ratings will carry less weight in reputation assessment.

Yu et al [104], [105], [106] further proposed referral systems using a weighted majority technique to belief mathematical function for aggregation to detect deceptive ratings. This work focuses on the problem of deception in testimony propagation and aggregation. The information stored by an agent about his direct interactions is a set of values that reflect the quality of these interactions. This approach calculates trust value of an entity based on the forgetting approach, in which only the most recent experiences with each concrete partner are considered for the calculations. Many other models were proposed using the similar weighing approaches of including forgetting factors when calculating trust such as [11], [12] and [50].

1. The limitation of both the approaches is the credibility of ratings received from other third parties. The network is not capable to distinguish between honest and malicious agent. They do not fully protect against malicious ratings

generated by malicious parties. For some reasons feedback providers are deliberately provide untruth ratings about an entity. As these models rely on other third parties to provide feedback ratings we must not assumed that all providers are trusted and are creditable. Nevertheless, both of the approaches do not address the problem of malicious ratings' providers who may intentionally distribute unfair ratings in order to achieve their financial gain.

2. The method used to evaluate trust value is only effective when the providers are truthful and all of the feedback ratings are creditable.
3. On the other hand, the weighing method may be applicable in conjunction with other mechanism for trust evaluation. For example, applies weighing method to both the majority technique and aging technique.

2.5.3 The Fuzzy Logic Approach

Different from Boolean logic which can only handle values between "totally true" and "totally false", fuzzy logic is able to handle the concept of partial truth. Fuzzy logic reputation trust management models make use of fuzzy logic functions to express the degree of trust of an entity that is between trustworthy and untrustworthy. The ReGret reputation model is one of the examples proposed by Sabater and Sierra [80] using fuzzy logic to determine trust.

ReGret is a decentralised eCommerce trust system proposed by Sabater et al [78], [79], [80]. This system used fuzzy logic approach for modelling trust and reputation. First, the agents are organized as and work in groups and each group have its buyers and sellers. The ratings of a selling agent provided by other members in a buying agent's group are also used for trust evaluation. This model incorporates parameters of direct experiences (personal interacts), information from neighbourhoods and system information to predict the trustworthiness of target sellers. Fuzzy logic rules are used by participants to ensure that the recommendations are not biased or incorrect. It takes advantage of a variety of information components and takes into account the social dimension of agents and a hierarchical ontology structure. This model based on three different types of reputation and combined to them to *ontological dimension* of reputation. Direct ratings or subjective reputation of an agent received from service provider is name as individual dimension of reputation. These ratings are weighted according to the recency of the rating. *Social dimension* is the estimation of the of trust value of service provider which is necessary when there is lack of direct interactions and for the new comer of the system. *Witness reputation, neighbourhood reputation* and *system reputation* are three parameters that are taken into account when evaluating the reputation of the *Social dimension. Witness reputation* are calculates from the ratings provided from others members who have prior interactions from the group. *Neighbourhood reputation* is calculated from social relationships of the individuals who are the neighbours with the agent.

1. Fuzzy logic based rules are use to compute the aggregated reputation of all the group members and the reputation value of participants is decayed with time functions. To adapt the dynamic nature of reputation in eCommerce environment, the weighing scale is necessary. It considers only the most recent impressions by using the time forget factor that allows reputation of participants decayed with time passes. This is an important factor as the

dynamic characteristic of an open online environment, behaviour of participants may influence by many other factors and do not always remain the same. This weighing method may be applicable in conjunction with other mechanism for trust evaluation.

2. ReGret diminish the problem of sparse ratings for trust evaluation, it allows newcomers who have no direct experiences with the others to take part in the community by using neighbourhood social relationships. On the other hand, neighbourhoods may not want to provide ratings or start new relationship with new comer as new comer may not necessary a genuine participant as new identity can be created when bad reputation built up.
3. This model relies on social relations with third parties via fuzzy rules to measure the influence degree of recommendations. However, there is no detection of any untrustworthy third parties and that the recommendation from the third parties may not creditable. It is important to know how reliable are the feedback ratings (recommendations) received. These unreliable feedback ratings affect the accuracy of reputation value.
4. Creating false identities may give user themselves away from connecting to their friends from their social network.
5. This approach is not able to diminish from the collusion. Any group of the agents have opportunity to collude and provide malicious ratings.

In summary, there are several characteristic that can be highlighted from the discussed trust management systems: a) Effectiveness of trust management system is dependent on the accuracy of trust prediction. b) The trust prediction is affected very much by the quality of the feedback ratings. c) All the discussed approaches can not fully combat the problem of feedback ratings deception and thus affect the accuracy of trust value prediction. The following Table 2.1 shows the summary of the reviewed approaches.

Table 2.1 Summary of the selected trust management system

Researcher /TMS	**Year**	**Model/Evaluation method**	**Model's Limitation**
eBay [31]	*2011*	-Centralised system, -simple summation	-Easy to implement but not flexible. -unreliable feedback ratings - feedback eliciting issues. - identity issues.
Amazon [3]	*2011*	-Centralise - average summation	- unreliable ratings - similar issues as eBay
Collaborative Filtering [99],[107], [111]	*2004, 1999, 2007*	-Centralised storage -User profile similarity - weighing scales	-Prediction difficulty. -Unreliable reviews - ratings insufficient -collusion issues
BRS [50],[51], [53]	2002, 2006, 2009	- centralised. - Bayesian model - Weighing scale - Forgetting method	-Flexibility and simplicity. -The discounting and forgetting factors are not sufficient
Travos [99]	*2004*	- beta distribution -forgetting and longevity -confidence metric and reliability - Majority ratings	- issues of feedback credibility
ReGret [78],[79], [80]	*2002, 2004*	- decentralised system - *Neighbourhood* -Fuzzy logic	- credibility issues - false identities -Collusion by groups

A multitude of trust management proposals have been developed, applying a wide variety of different mechanisms, techniques or approaches. Their aim is to try to manage the problem of online fraudulent activities that restrict the growth of eCommerce. The trust systems described above are some of the current research into trust management system. These proposed systems offer advanced features aiming to design a constructive decision making tool in an uncertain environment for eCommerce participants.

These trust models capture the evidence necessary to characterise the nature of an entity in terms of trustworthiness. Trustworthiness was evaluated according to the direct and indirect knowledge on earlier interactions of entity with a particular entity. Many other contextual elements such as interaction times or frequency, role of entity, time decay and context similarity were included in the evaluation process. Some of these models used mathematical functions to evaluate trustworthiness, support important of weights of different factors. The weights are representing the influencing relationship among these factors and the trustworthiness. These evidences can be aggregate according to both centralised and distributed methods. However, the existing work did not give a common consideration on all factors that influence trust. Most of these proposed models have only considered simple factors during the evaluation processed. Trust is important in decision-making and that the characterisation of an entity must capture more complex parameters [51].

2.6 Chapter Summary

This chapter covers some of the trust and reputation challenges involved in eCommerce trust management system and how these challenges being solve by the current work. It presented the background of trust management system and introduced previous work done on trust and trust management is presented in the literature. The literature review of trust management systems shows that reliable reputation systems still remains a challenge. Current works lack a practical approach that could help us in the design and development of a usable trust management system.

Moreover, techniques of trust assessment need further improvement in order to enhance the current eCommerce trust management. First, an effective technique to verify the reliability feedback ratings from participants of eCommerce urgently needed. There is typically an assumption that feedback ratings are truthful and unbiased, which may not always be the case. Applying an appropriate filtering technique to the collected data would help trust management system made their transactions smoothly and safely.

Second, existing work on eCommerce trust system often compute trust based on overall performance instead of individual service performance. That is the contextual relevance of evidence is not taken into account for trust evaluation. Third, the accuracy of trustworthiness or reputation measure is a concern. Trust evidence requires a formal evaluation scheme to represent the relationships between entities. Thus, trust evaluation schemes must accurately reflect the contributing evidence. This is to ensure the trust relationship established for an intended purpose and sustained until the purpose is fulfilled. The discussion and understanding gained from the literature study helps our work towards solving special issues of trust and proposed new schemes in the coming chapters.

Chapter 3

A Multilevel Trust Management Framework

It is important to develop an effective trust management system that assists eCommerce participants to make trust decisions. This chapter proposes an approach towards such a system, which gives a better understanding of the components that can be used in a trust management system. It identifies and illustrates the components contributing to the trust making process. We introduce a multilevel trust management framework to improve ways on trust management in eCommerce environments. We describe the desirable properties of a trust management system and analyse security threats to a trust management system. This framework considers a number of factors that may influence trust relationships among buyers and sellers. It includes feedback from buyers' recommendations and system trust. We also conduct a case study on how to improve buyer-seller trust relationship in an eCommerce application using the trust model.

3.1 Introduction

In this chapter, we address the problem of feedback-related trust management systems vulnerabilities. A feedback-driven trust management system is widely adopted in eCommerce marketplaces. The aim of the a management systems is to manage the trust relationships between business partners. This is achieved by maintaining the trust-level of the eCommerce participants and makes them available to potential eCommerce customers when needed. The trust level is derived from feedback ratings submitted by the trading partners after the successful completion of the transactions. The submitted feedbacks are analysed, aggregated, and made publicly available to the interested parties. The trust values accumulated from the past transactions information provide important reference for future users. Both buyer and seller judge each other's credibility by their trust values. Establishing trust is the way to build good relationship with both buyer and seller which positive activates will increase trust level, otherwise destroy trust immediately. Since trust value must be determined based on past experience from both buyer and seller, establishing an initial trust level can be a major challenge to both potential buyers and sellers. It's also clear that without initial trust, sellers cannot build a good transaction history, and buyers may not build trust in these sellers. The other question concerning eCommerce management systems is equations do not accurately reflect trustworthy of transaction partners (buyers and sellers). It is hard to evaluate and exchange reputation between eCommerce users due to the differences in perception, calculation and interpretation. But most of all because the given reputation is calculated based on overall transaction information with different quality criteria or attributes , it does not reflect the related contexts. In recent years many researchers have focused on trust related issues but there is not a unified and broad framework for trust. Without providing a unified and broad framework for trust, it is challenging to define suitable trust management model for eCommerce. Therefore, an effective trust management system needs to be designed to meet the complex requirements of real-world eCommerce applications. A trust management system that is able to maintain trust relationships and build initial trust will be valuable to establish trust between buyers and sellers. A trust management system depends on several information sources to build initial trust from collect off-line transaction histories, trust value, system security, and available to track transaction histories and other information. The fundamental criteria and requirements for eCommerce trust models to follow are still not well understood. Two problems need to be solved herein. Firstly, an ideal trust management is needed to improve the support for existing trust management in eCommerce. It should provide essential security services, such as to validate the identity, provides services, secure storage, privacy support and provide an efficient and effectively trust decision tool. Second, the model must be accurately predicting the trust value of interactions success. Trust model must be able to maintain accuracy even under dynamic condition, adapting to changes introduce by others.

Finding a reliable trust modelling methodology is essential, and thus by applying the model to build up a trusted system. The current trust management system is lack of a consistent model to help managing trust.

To satisfy these requirements, the following section addresses the need to be considered.

3.2 Trust Managements System Requirements

This section addresses the requirement of an effective trust management system.

3.2.1 Accuracy of Trust Information

The accuracy of trust value means the correctness or truthfulness of trust information. This also means the estimation of trust value of users is accurate at the time of evaluating. Much of the information needed to compute trust value can be gathered from various sources as mentioned earlier. This information could be accurate or could be designed to mislead the user into falsely trusting the seller. Accurate estimation is crucial for trust management system as accurate trust information improves trust relationships between businesses and end users, as trust between businesses and consumers are crucial to the expansion of eCommerce. On the other hand, inaccurate trust information leads to misinformed business decisions, resulting in poor judgment and bad business outcomes. Trust information can be improved if each user shares her experiences about aspects of the level of services provided by the users she interacts with are truthful. Therefore, the user would like to ensure the accuracy of the supplied information so that trust the party that can be trusted. The main problem when attempting to give users accurate trust values are that the trust information is too general. It provides one single trust value to represent overall services of a seller, but does not specify the trust information of the product which the buyer acquires. Transactions in the same amount category can be considered relevant when evaluating a transaction trust bound to a new transaction. For example, a seller may not good in service “A” but excellent in service “B”. Thus, the previous transactions in the same product category should be considered as one of the factors in trust evaluation.

Trust assessment requires gathering more information such as to compute trust information that is represented different services of a seller. Another issue is in online eCommerce environments, the reliability of the trust management system depends on numerous problems such as falsified and biased ratings [47], [60]. The intention of falsifying rating is to inflate or deflate a vendor/buyer’s reputation. Falsified feedbacks can compromises the reliability of the trust management systems and seriously affect the trust level of good sellers. While trust management systems are increasingly being used in eCommerce environments, they are susceptible to tampering with ratings. For example, a small percentage of falsified ratings could degrade the accuracy of the trust level, compromise the overall trustworthiness of the participating parties and render the trust management system unreliable. While it is impossible to expect all rating providers to provide actual ratings in an open environment such as e-Commerce, it is necessary to have an approach that is able to detect falsified ratings to protect the integrity of the trust management system. Although there have been techniques to encourage trustworthy behaviour [58], [25], [97], the general trend in trust management system is to consider all ratings as accurate. Unfortunately, since the trust management systems rely on the rating provided by the trading partners, they are frail to strategic manipulation of the rating attacks. Hence, mechanisms to identify and action falsified ratings and an efficient trust metric that includes all necessary factors is required to improve the current trust assessment techniques.

3.2.2 Scalability of Information

There are definitions about scalability in many fields [52], [60]. Based on the definition of scalable system, the scalability of trust management system is when the system parameters change, such as increasing of user number (buyers and sellers) and resources, it does not lead to the decrease of system performance. Thus, we consider the scalable system as the trust system can deal with the increase of users and increasing of trust functions without decreasing system performance. As the number of parties involved in transaction increases, the number of direct and indirect experiences increase. In addition, when the interaction about different services increase, the trust information request may increase and increase its complexity of the system to obtain information. Moreover, to keep level of trust value updated, any changes of value from information source which is direct and indirect interaction must be used to update the trust value immediately. The trust management system should have the capability to change dynamically in many different ways that could affect the trust values of different users without changing any other interaction details.

A scalable trust management system is necessary as the load of eCommerce transactions grows to millions of transactions. Its processing power should be able to grow quickly, providing throughput and reliability. To make trust management system scalable, it is necessary to study: the storage of trust information, the transmission of the interaction data and the feedback ratings information. Delegation is an important mechanism that can be considered for improving the scalability of trust management.

3.2.3 Availability

Availability is the percentage of time when information needed. The information required to build trust is also based on the availability of a service [16]. The low availability constrains the areas available to make transactions. This may require some information about the reliability of all the related services. A trust management system must be able to support combination of feedback ratings from multiple users. In order to support high availability the trust management service, all history records managed must also become available for trust level evaluations. It also should support the use of different trust evaluation functions by different users over the same feedback ratings from a completely distributed eCommerce users. The accuracy is improved by ensuring that all of trust information and all components involved are available. The problem of achieving this remains unsolved as trust management involves data collection, analysis, trust establishment and trust monitoring, etc.

3.2.4 Security

Security refers to data protection in e-transactions, and is recognised to be a fundamental component in eCommerce as eCommerce has led to a new generation of associated security threats. In the studies dealing with trust framework, protection against malicious attacks and recovery from attacks were highlighted [13]. Security mechanism of eCommerce trust management system must meet the integral requirements in order to establish secure eCommerce transactions. These requirement including authentication (identities of transacting parties are genuine), confidentiality (transactions information are kept from unauthorized parties), integrity (transactions are not compromised) and the external security threats, availability (transactions are available by relevant parties when needed). As eCommerce customer accessing information relies on online trust management system, supporting the availability, integrity and confidentiality of this information is crucial. It is difficult, if not impossible, to complete a transaction without revealing some personal data, such as shipping address, billing information, or product preference. Users may be unwilling to provide this necessary information or even to browse online if they believe their confidential information is invaded or threatened. eCommerce trust management systems need to ensure users can securely store critical information, ensuring that it persist, continuously accessible, unchangeable and confidential. Effective countermeasures should be studied and seamlessly integrated with the design of trust management systems.

We have briefly introduced the need of a trust management system in section 3.2. This chapter describes how these objectives are met in the multilevel trust management system (MTMS) framework and provides a brief and informal overview in the next section.

3.3 Multilevel Trust Management System

Figure 3.1 illustrates the structure of the multilevel trust management system (MTMS) framework. It encompasses four components: a data collection, feedback verification, trust evaluation and data management level.

In figure 3.1, a security framework including an access management closely collaborates with all the other components to offer security related management. A data collection component is responsible for recording all useful information about ratings received from participants for trust assessment. A feedback verifier is composed of a number of verifying schemes to predicate suspicious feedbacks such that the impacts of such feedbacks on the computation of trust level could be minimized. A trust evaluator is teamed up with the verifier to conduct trust assessment and trust establishment by requests from other frameworks. It combines information from the verified ratings and the ratings history of users. A data management is to manage the trust data storage, retrieve, distribute and to collaborate with look up and update components to contribute toward securing data management practices.

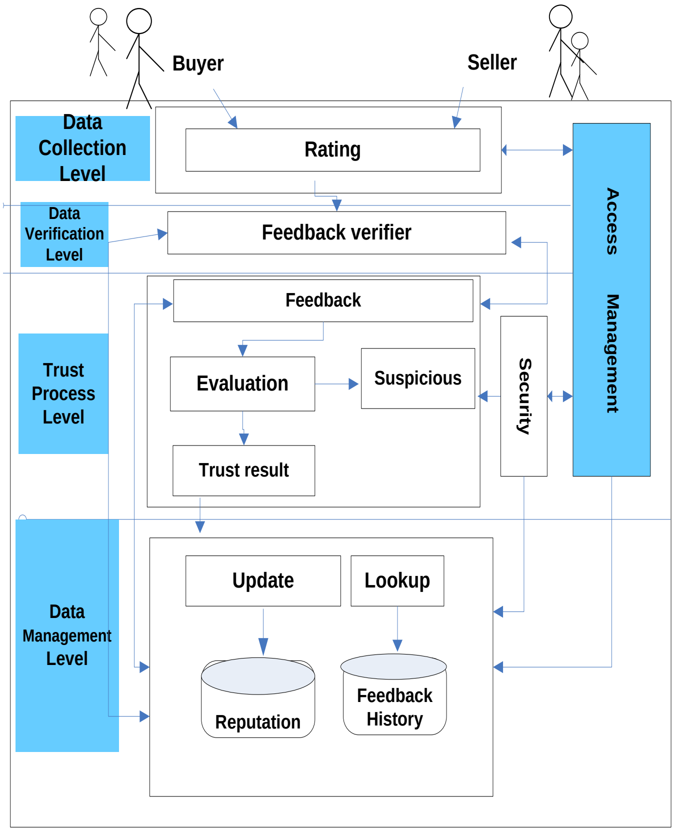


Figure 3.1 Multilevel trust management architecture

3.3.1 System Overview

The following sub section explains the overview of each component of the MTMS.

3.3.1.1 Data Collection Component

As shown in figure 3.1, a service can conceptually be broken up into several components in which the interaction between buyer, seller and trust system via the interface. Initially, buyer searches specific product information. Buyer enquires the trust value about the seller of the specific product. The request is sent to the trust system. The request will be shown to the buyer once the authentication and authorization process are successful through the authentication and access control mechanism. The conditions on which such requests are granted are specified by a local policy. Upon a request, the access control mechanism constructs and sends corresponding policy queries to the evaluation engine. If the answer is positive, the request is granted.

The initial trust value is accepted by both buyer and seller before their interaction. The buyers will rate the quality of a service after the transaction is successfully completed. The trust system uses the ratings received from the buyers to determine the trust level of the seller. A data collection component records a collection of service history. For the purposed of identifying ratings to the corresponding services, each service invocation history record consists of the following fields: user Id that initiated the transaction, service identity (ID), service type and time invoked by user during the transaction. The creating of service history records from the performing by MTMS are created and reported using the following steps.

1. If a buyer B completes a transaction with service S, S creates a service invocation history record H.

   H = (B, S, FV, DT).

   a. FV is the transaction rating value given by buyer B.

   b. DT is the date and time service.

2. The record H will not be created until FV and its associate's attribute can be completely determined. For example, the buyer did not send payment to the service, which would affect feedback for the transaction.

3. Once service invocation history record H has been created, service S reports H to the MTMS. In the service infrastructure, each service S has a partial

view of buyer B behaviour based on its interactions with each buyer. By reporting feedback to the MTMS, each service reports feedback on these interactions to the MTMS when needed. These feedbacks are then supplied to the feedback verifier. Each aggregate feedback is then be available for trust level evaluations by all services.

3.3.1.2 Feedback Verifier

An effective verifying scheme, which is able to verify and mitigate various feedback related threats to the feedback ratings collected, enhances the accuracy of the estimation of trust scores. The following demonstrates the verifying process of determining the rating credibility.

a) Once the verifier receives the rating, it validates the rating ID. The ID is only valid when the users are active in the system. It is considered invalid when the users have not been participating in the system for a specific period of time. This is to avoid any rating coming from fraudulent parties. As it is unique to every user, the feedback ID can uniquely identify an individual. Therefore, the verifier could identify whether the rating is from a true or valid provider. Then the feedback verifier looks up the feedback provider’s business profile, including the business details through the history database. Combining with associates parameters, a mathematic verification function is used to determine the weight of the rating.

b) The Feedback verifier gets the rating history through the lookup mechanism. The rating provided is compared with the ratings history.

These histories alone are insufficient to justify the rating credibility. The trust value of the seller is included in the scheme.

c) The Feedback verifier retrieves the trust value information of the seller. Depending on the rating history and the level of trust value of the seller, the rating is assigned with a credibility value, and the credibility values of ratings are sent to the rating database which stores the verified ratings.

3.3.1.3 Trust Metric

The main functionality of trust metric used by trust evaluation mechanism is to provide a trust value for users. Trust value is the result of trust evaluation. There are several existing mechanisms that can be applied for assessing trust through past history[76][77]. We develop a trust metric scheme which consists of verified ratings to evaluate trust. The trust metric evaluates user trustworthiness based on the verified current rating received from users after a completion of business transaction and the past behaviour of a user which is represented as a collection of service history records.

The following steps illustrate the process of evaluating trust value of users based on our trust model performing by MTMS.

Whenever the system receives a service request from some users, the system send its custom trust level using its trust function defined over a collection of service history records along with the feedback identifier to the MTMS.

1. Upon receiving feedbacks for some service, the verifier of MTMS computes feedback credibility over the collection of service history records and return the resulting to feedback storage.

2. MTMS computes the trust level of seller S based on these verified feedbacks using its trust evaluation mathematic functions. The trust evaluation offer trust status directly relevant to the product that the buyer is going to purchase.

3. MTMS uses trust evaluation factors including rating value, past history, time, product information (such as types of product, cost and warranty) and weighing scale to estimate trust value for each user.

3.3.1.4 Trust Data Management

Upon receiving new trust information of users, the trust information is update from the MTMS by lookup and update mechanism. In this work, the information regarding trust relationships between buyers and sellers is kept in a trust database. The trust relationship, the users' information, the parameters to evaluate trust, and the access policies are represented as relational entities. All these are translated to tables of the database and the attributes of these entities are expressed as columns in the tables. To prevent overloading, the amount of previously evaluated trust value is deleted based on the recent activity of the services. If inactive service is above a set time by the system, the lookup mechanism checks each service and its membership. Both trust information and the membership of the service will be deleted and then updated.

Trust information has to be kept highly confidential and to maintain its integrity. This means it needs to enforce some form of security mechanism such as access control, credential mechanism, and encryption. When buyer visits seller's web application either login as a user or registered as a new user. Users are authenticated through user id and regular password mechanism. Users are assume with two different roles namely seller or buyer. User ID and password information is passed to authorisation entity to validate members' ID. If this information and the login table are matched, users are allowed to access the system based on the access control rights they have. If user is new to the system, a registration process is needed in order to register user as a new user to the system. After the authentication process of matching the information is successful, user is authorised to access the trust information of the data storage. The requested trust information of seller is shown. The goal of the access control is to admit only authorized personnel to a particular location. Authentication process relying on one or more authentication factors in an identity-based transaction constitutes an authentication method.

The following algorithm is used to compute the trust relationship with a seller for a given context at any given time.

1. If not already a user, initialize the buyer's information corresponding to the seller and the specific product. If needed, update the same to reflect current circumstances.
2. Initialize access policy with buyer if not already available. Update as needed.
3. Compute credibility of a rating give by buyer
    (a) Read provided rating value
    (b) Read seller trust values from database starting from most recent first of a history table.
    (c) Read buyer trust values from database starting from most recent first of a history table.

(d) Read information of product interaction.

4. Compute trust value of seller
    - (a) Determine last activity in time when trust is evaluated for current seller for the given product.
    - (b) Read trust values from database starting from most recent first of the history table.
    - (c) Read rating values obtained in steps 3.
    - (c) Apply product information to evaluate current trust value.
5. Record current time of trust evaluation.
7. Compute decayed value
8. Combine trust values obtained in steps 4 - 7 using the weighing factor to get seller’s current trust value for the given product.
9. Trust information is updated

In addition, implementation of a security defense system [19] shows it can protect services from distributed denial of service (DDoS) attack and improve system efficiency. The framework is distributed on each router in the network so that it can provide overall protection. Each Bodyguard is a destination end protector, it provides security as the traffic enters the network. This security framework allows bodyguards to send updated security information to each other (new attacks that each has encountered, for example). it also sends security information down to the next hop for checking application data as it comes into the router (This is to provide better performance, by breaking up the security and application data) and lastly, monitors the performance of each other (So if a successful attack brings down a bodyguard, the next hop router is prepared to handle the security). In general, the main component of the security defense system, which consists of the following objectives: 1) mitigating the problem of distinguishing between normal and DDoS attack traffic, 2) protecting the system, while allowing other applications to run at their full performance potential. 3) Minimising the effect to the performance of applications when there is an attack. Although, system security is not in our focus, the implementation of security mechanism helps improve the effectiveness of trust management in eCommerce. Further investigating into performance over a practical implementation of this framework is required.

3.4 Examples of Trust Relationships

In this section, we illustrate two Examples, an online book store similar to Amazon [3] and a travel referral service, Zacasso [112] in the real world to assist trust building in an eCommerce system for the MTMS. These examples are helpful in understanding the properties of trust relationships expressed in section 3.2.

Example 1: *An online book store calls AAA.com which operates as an online retailer internationally. It offers programs that enable sellers to sell their products on company's Websites. In addition, the company provides fulfilment* services; *miscellaneous marketing and promotional agreements, such as online advertising; and co-branded credit cards. International book is one of the book stores selling its product through AAA.com.*

Alice logs onto her computer, accesses an internet site "AAA.com" search for a book title "Foundations of Medicine". This book is available at several different sellers. She decides to purchase it from a seller who has high rating of 96% positive called "International book". The book costs $250 plus a $10 delivery charge. Alice pays with her credit card and is told her book will be delivered in 5-7 business days.

This simple example involves a service-oriented system in the "AAA.com" setting, assuming that they are conducted over computer mediated networks. These processes include electronic marketing to reach Alice, and electronic search to find the book's title and book seller "international book", electronic procurement and payment to obtain the book from its whole seller, electronic authentication of Alice's credit card information, electronic processing to obtain payment from a financial institution, electronics shipping arrangements for delivery of the book, and electronic customer support to e-mail Alice an acknowledgement, order number and expected delivery date. Understanding the effects of these processes on “International book” of its operation and cost, its supplier and customer relationships, and its competitive industry position are a significant measurement challenge. This example demonstrates the business to consumer transaction involve a larger number of related business to business transactions. These include Alice’s purchase of book from “International book” and the “International book” separate transaction with third parties to obtain order fulfilment services. Acquire the book for release, secure credit authentication service, provide payment processing services, and arrange for delivery of the book to Alice. Thus, “International book” who is both a seller (to Alice) and buyer (from a supplier)

Some of the trust relationships involving buyer and seller are:

1. AAA.com and seller trust buyer to responsibly search, view and make purchasing through their web system.
2. Seller trusts buyer for the payment of the purchased
3. When making decision, buyer Alice trusts AAA.com and belives the seller’s information of trustworthiness is accurate and updated.
4. Buyer trusts seller kept her personal detail in a secure database.
5. Buyer trusts seller to send the book within 5-7 days according to the agreement.
6. Buyer trusts seller to send her the book purchased is exactly to the description.

7. Seller trusts the payment service providers kept his information in a secure databases.
8. Seller trusts the payment service providers to collect payment from buyer.
9. Seller trusts its third party to delivery the book to buyer.
10. Seller trusts buyer to provide genuine feedback about the purchased.

Example 2: *An online eCommerce service Zicasso [112] is a travel referral service that connects buyers (travelers) with sellers (travel agencies and tour operators), somewhat like eBay being a marketplace that brings buyers and sellers together. Travelers and vetted travel specialists work with each other, as members of Zicasso's trusted community, to define and refine the ideal itinerary. Zicasso is a free service for travelers means the buyers (travelers) do not pay to use the service but a small amount is charged from the sellers (travel companies) same way in which eBay and Amazon.com Marketplace make money. Zicasso functions as a marketplace for Travelers and Travel Companies to facilitate travel transactions between Travelers and Travel Companies. The Site provides tools to facilitate transactions between Travelers and Travel Companies.*

Similar to the Example 1, user logs onto her computer, accesses the internet site of "Zicasso" search for a best travel deal to a specific destination. A few travel company services agent provide the same services that meet user requirements. User selects the travel agent service provider and accepts a trip plan and purchases based on their rating.

Some trust relationships involving Zicasso and their service providers are modelled as:

1. Zicasso trusts the service providers is a genuine user of it system.
2. The customer trusts Zicasso to provide trust information of service providers (Travel Agent).
3. Customer trusts travel agent provides services that meet their holiday requirement.
4. Travel agent trusts customer when they have address details and confirmed credit card information that makes their purchase.
5. Travel agent trusts customer provides genuine rating after the service.

The above is a snapshot of (some of) the trust relationships that exist in these two applications. Central to first Example is the exchange of trust information between all parties: Alice, “International book”, its supplier and its third party payment service provider who is a seller of services to “International book” and Alice Credit Card Company. As a consequence, managing trust and information confidentiality settings between all users of the system increases in complexity. There are elements of choice at both ends of the process: Alice wants to be able to choose from a selection of suitable seller, while seller wishes to choose from a selection of qualify customers. Protection the release of information from both Alice about herself and the seller help ensure fairness throughout the process.

First, “International book” has to present a number of credentials to prove its trustworthiness to his whole sellers, whereas buyers base their decision on past performance of the service (experiences of other buyers). The seller, “International book” plays a key role in this Example, as Alice’s personal information needs to be exchanged among the seller’s third party payment service provider and Alice’s credit card company to match Alice information. To specify risk profiles, the set of actions that is to be used in the trust and recommend specification must be known. Below we present the steps in the Example relevant to Trust Management.

In the first Example, a potential buyer (Alice) goes online AAA.com to search for a book wants to buy from a suitable seller.

1. The potential buyer searches for a trustworthy seller which is rated by buyers based on their experiences they have had of the service.
2. The potential buyer searches for another seller if the chosen seller site is not available.
3. A username and password to access the system are given. At this point a basic contractual agreement is established. Potential buyer is granted access to the system.
4. Buyer makes decision to purchase from seller.
5. The payment to the seller is paid once the procedure of purchase is completed.
6. Buyer provides her personal detail, e-mail address and credit card number.
7. The seller transact with third parties to obtain order fulfilment services. Such as secure credit authentication services to verify the potential buyer’s identity, checks if she is trustworthy.

8. Buyer information is used to match her profile with the credit card number provided. The matches are collated by the payment service provider and the buyer’s credit card company exchanges buyer’s personal information, as well as provides payment processing services.
9. The seller tells the buyer her purchased is accepted through e-mail.
10. The seller arranges for delivery of the book to Alice.
11. The buyer will have to wait for the book to arrive in 5-7 days.
12. After the process is completed, the buyer has the opportunity to give feedback on the service by rating different aspects of the service, such as speed or quality.

Buyer decision is made based on the seller rating information and she believes it is accurate. Buyers’ sensitive data, such as buyer personal details, needs to be shared among seller and payment service providers, for example when verifying for information about the credit card holder. Our case study shows how trust can be established and how it changes dynamically based on updates to the trust information. Since the data that is used to establish trust may itself be sensitive, we also discuss the trusted system security requirements and implications of the trust framework.

Due to the similarity of the first Example, we omit the discussion of the steps in the second Example relevant to trust management.

3.5 Validation of the Framework

In this section we validate the framework by applying it to the real online retail book purchase and the travel agent in section 3.4, and showing the different trust needs. Our focus is on the trust requirements imposed by both of these examples. We discuss how individual component contribute to a trust management system.

3.5.1 Trust Information

A data collection, feedback verifier and trust metric are three important mechanisms responsible for evaluating trust information. Feedback ratings are received from buyers at the data collection level. Feedback rating verifier filters these feedback ratings to ensure the credibility of these feedback ratings. All filtered feedback ratings are used to evaluation the trust value of the particular agent using an evaluation scheme.

In this trust management, the decision of a buyer whether to trust sellers on their services is based on own direct past experiences, or from others or from both direct experiences and others experiences. Sellers have to present a number of credentials to prove its trustworthiness to the trust system. Now, let’s consider the scenario for this trust management system. We apply the threats model to the scenarios. There are two types of possible threats concern to this component: Unreliable feedback and inadequate evaluation technique. A data collection component collects ratings from both buyers and sellers. Buyers are able to repeat their buying process as many times as they want. Every time when a buying process is completed they are allowed to provide feedback ratings. Buyers may not provide truthful feedbacks. These feedback ratings may not be creditable to evaluate provider trustworthiness. As many there are many sellers are with the trust system, buyers may receive incentive from other sellers to provide feedback ratings. Another possibility is that these feedback ratings may have been intercepted by other users with unfavourable intention. If these ratings are used to evaluate the trustworthiness of the seller, the result is not truthful.

Our proposed model the data collection level includes feedback verifier and trust evaluation mechanism. Feedback verifier verifies the feedback ratings to ensure the credibility of feedback ratings. The trust evaluation mechanism evaluates the trust worthiness of the users using trust metric based on these filtered feedback ratings and several other trust factors, such as time decay and product information. More importantly, this metric provides a trust value for new seller who has no past history to build initial trust with buyers.

3.5.2 Data Management

Data management is to maintain the trust data up to date and provides most recent information to both seller and buyer.

The proposed data management component necessary to manage the storage, retrieval, and distributes the trust information in a scalable and efficient manner. In the examples given in section 3.4, buyers are allowed to register with many sellers within the trust system First, a potential buyer looks for a trusted seller or sellers. Based on the trust information provided, she makes a decision to which seller she would like to interact with. She may make decision based on the trust information and her own risk perception, e.g. she trusts a seller if the trust value is more than 9 out of 10. Others may trust a seller if the trust value is 7/10. The look up and update mechanism is there to help the trust system prevent data overload and maintain the efficiency of the trust system. The trust metric includes a time decay factor to delete unnecessary information to maintain the accuracy of trust values of different users without changing any other interaction details. The lookup and update component is needed to monitor whenever it is a change to the trust information. If the trust information has not updated and is not the recent trust information, buyer may have made a wrong decision as the trustworthiness of sellers may have changed. The potential buyer can repeat the process if no suitable seller is found. It is possible that buyer's information have changed since the last process. If buyer's new profile has not updated, the matching process may not succeed as her profile is remained at the previous status. The proposed data management mechanism is necessary to update her information to avoid any confusion. Processes must include secure operations. Obviously, trust information has to be kept highly confidential and maintain its integrity. This means it needs to integrate with access management and some form of security mechanism.

3.5.3 Security Mechanism

A strong authentication and authorisation mechanisms must be used to ensure only authorised users have access to the trust system. In both of the scenarios, sellers need to sign contract with the trust system. During this process, one of the trust requirements given by the seller is a number of credentials.

Sellers need to access buyer’s personal information of buyer. Buyers need to access to the trust information of sellers, the credit card detail of buyer. Protect information integrity and prevent information disclosure from any unauthorized users. This means it needs to enforce some form of access control such as, policy, credential mechanism, and encryption. This is to ensure the trust information maintain its integrity and prevent competitors to have any access to it. The access policy is used to determine who has the privileges to access which information storage. As the same time, access control management mechanisms have full responsibility to trace the misuse of the system back to the responsible users.

In the description of both scenarios, the availability of information need to be 24/7 as the sellers and buyers are located internationally and many different sellers are with the same trust system. The availability of information is crucial for this trust management system. Buyers need to access information from seller or sellers if information is not available at a particular time, they may move on to another available seller. Sellers need to respond buyers’ enquiries on time. Any delay causes inconvenience on both parties. Sellers need to access trust information from trust system to provide feedback to buyers’ enquiries. Therefore, other than a effective trust metric, a system security mechanism is also needed to guard against unauthorised access to the host or network. Strong access control policy also assures the validity of a transaction and user. Users are unable to deny that a transaction is occurred at a particular time.

In both the scenarios, buyer are required to provide personal detail including their credit card information to seller/sellers if the purchases of product is successful. If transaction is successful payment is made to the seller/sellers. With the strong access control mechanism, seller/sellers are unable to deny of receiving the ordered from buyers. Also, seller/sellers are unable to deny the acceptance of payment from buyers. On the other hand, buyers are unable to deny that seller/sellers have already send the purchased products, and buyers are unable to deny provided a particular feedback ratings to seller or sellers.

3.6 Chapter Summary

Understandably, there is no single solution to mitigate eCommerce risk. Although there has been a significant number of works in trust management, there are still some open fields that need further exploration. As trust may depend on many different factors, in a flexible eCommerce trust management, trust must be computed by combining different types of information. Using this combination, we introduce a multilevel framework for a new interactive trust management to improve the correctness in estimate of trust data. Such a trust management system would calculate trust value based on what buyer want, and provide the best trust information according to the buyer's requirements. This chapter studies and examines the importance of the trust factors of the trust management framework, specifically in dealing with malicious feedback ratings from eCommerce users. In this chapter some desirable properties of an ideal trust management system are addressed. Value added access management and a security mechanism are implemented at all levels, meeting all requirements that a trust management system should support. We envisage that this proposed framework increases consumers' trust and encourages consumers to increase their participation in eCommerce. The main advantages of the proposed trust management solutions can therefore be summarised as follows.

The proposed multilevel trust management allows unknown parties to access services by showing appropriate credentials that prove their qualifications to get the services. The approach facilitates dynamic updating of trust information to reflect the current or latest behaviour. Also, the decision making is entrusted with the individual user that takes decision based on its own experience and all on the information received from the users. We also show that a trust management system with only one component (e.g., trust value) does not cover all the necessary functions and services. Moving beyond simplistic and vague applications of the notion of trust, researchers are enabled by this framework to recognise when trust is relevant and to address a broader range of elements and process involved in trust assessment. How to merge the trust relationships into the overall eCommerce systems provides lots of challenges for further research. However, we believe that our proposed framework could be used as a helpful tool to model the trust relationships. The proposed required properties provide some starting points to develop a methodology for modelling trust in eCommerce.

Chapter 4

Enhancing eCommerce Trust Management Reliability

This chapter proposes an approach for identifying and actioning of falsified feedbacks to make trust management systems robust against rating manipulation attacks. The viability of the proposed approach is studied experimentally and the results of various simulation experiments show that the proposed approach can be highly effective in identifying falsified feedbacks.

4.1 Introduction

In this chapter, we address the problem of feedback-related trust management systems vulnerabilities. The proposed approach predicates suspicious feedbacks such that the impacts of such feedbacks on the computation of trust level could be minimized. The key contribution of this chapter is the design of an approach that verifies suspicious feedbacks with the aims of identifying and actioning feedback-related vulnerabilities such as those identified in [51], [58]. The proposed approach combines majority ratings and others parameters such as the amount of the transactions and the number of ratings submitted by a same participant to mitigate the re-entry and value imbalance issues. Our approach avoids such shortcomings as the normal ratings are separated from suspicious ratings. Also, instead of discarding suspicious ratings, a trust metric scheme is proposed to eliminate the issue of ratings sparse and discourage and reduce the impact of suspicious ratings.

Most of the proposed schemes depend solely on users' previous transaction history without distinguishing the relevancy of the services. On the other hand, we think this method is unfair to the sellers. Sellers who supply a good quality product may not necessarily provide a further product of similar quality. In a reputation system, it is necessary to assess the trustworthiness of sellers according to their service relevancy. In this system, the feedback of the seller is grouped into two subsets as relevant and irrelevant products or services. This allows us to select the right subset of ratings for trust evaluation. In other words, we obtained feedback from the relevant group in order to calculate the trust value. However, when no relevant ratings were found, we used the other ratings that were not relevant to the service sought. Initially a buyer and a seller’s reputation were set to 0. The reputation of both the buyer and seller was updated based on the assessment of ratings received about the transaction. This meant both buyer and seller built their reputation slowly based on their good performance which was rated by each other after each transaction. If they failed to meet the requirements, their reputation suffered.

4.2 System Model

The focus of this chapter is on business to commerce (B2C) model where both buyer and seller submit feedback after a business transaction is successfully completed. In this section, a generic architecture of trust management system is presented. Figure 4.1 shows a high-level architecture of an eCommerce system composed of buyers, sellers and products.

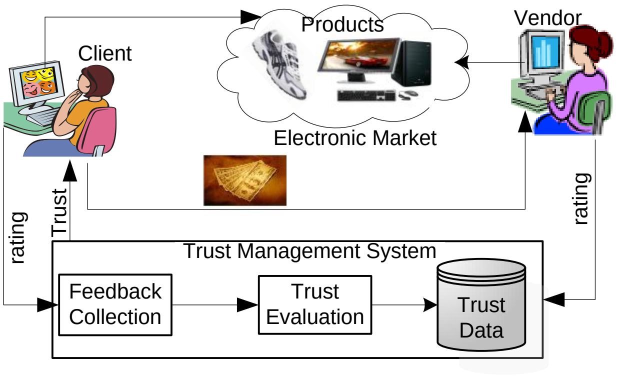


Figure 4.1: A generic trust management system

These components collectively cover most, if not all, phases of eCommerce business transactions such as orders and payments, marketing and distribution. They also enable sellers to advertise products and services, deliver goods and services, and provide ongoing customer support. These components also enable buyers to enquire about products and services, place orders, pay for it and receive goods and services online.

We assume that the sellers have web site that displays and describes to the customers all of the information about the products, prices, manufacturers, product warranties, etc. Buyers browse the catalogue of the merchandise, this can be using a computer, a PDA, a mobile phone etc to choose one or more products and pay for the order. This acts like an electronic shopping basket and it keeps a record of all of the things that you intend to buy. Once you have chosen all of your items, the payment processing components enable funds to be transferred electronically to anywhere in the world. Your order is then processed by the ecommerce store and sent to you by post. If a successful business transaction occurs, feedback about the service or product is collected from both the customer and the sellers. The collected feedback is then aggregated to produce a trust-level or reputation for both the seller and the buyer. The trust-level is then used to help potential buyers or sellers decide whom to trust and subsequently transact with.

Although eCommerce offers enormous opportunities for online trading, the open and anonymous nature of eCommerce presents potential risks to the online buyers. The trust management system will use the feedbacks received from the buyers to determine the trust level of the seller. In this chapter, it is assumed that each feedback is uniquely identified by a buyer ID, a product ID, a seller ID, a timestamp and a rating value between 0 and 1. The timestamp is used to verify the originality of the transaction and the actual time the feedback was submitted. Also, a seller/buyer is considered high value if his/her trust level is ≥ 0.8 and low value if his/her trust level is ≤ 0.2. Finally, a transaction value is considered high if the transaction amount is ≥ 0.8 and the transaction is considered of low value if the amounts to ≤ 0.2.

Transactions in online markets require a great deal of trust among anonymous trading partners. Most online buyers do not have much previous experience dealing with the same trading partner. When there is a lack of personal experience, buyers depend on information from third parties through eCommerce reputation based trust systems. It is imperative that reliable and effective trust models be in place to enhance the success of eCommerce trust system.

4.3 Feedback Verifying Strategy

The reliability of the system depends largely on the truthfulness of the ratings submitted by the buyers. In this section, we present an approach that try to detect and avoid falsified feedbacks.

4.3.1 Overview

A multi-attribute trust management model that incorporates trust, transaction costs and product warranties is discussed in [18]. The new trust management system enables potential buyers to determine the risk level of a product before committing to proceed with the transaction. This is useful to online buyers as it allows them to be aware of the risk level and subsequently take the appropriate actions to minimize potential risks before engaging in risky businesses.

We need to make few observations for the proposed techniques. We believe it is possible that malicious participants gain majority ratings through collusion. First, a trustworthy participant is more likely to provide trustworthy feedback [109]. Second, as identified by [38], the number of transactions is an important factor for comparing the rating in terms of degree of satisfaction among different participants. If the number of ratings submitted to a particular service by the same participants is increased dramatically, these ratings are more likely to be malicious than a scattered participant. It is because a participant could boast the majority rating by submitting as many ratings as possible. Third, the feedback of a transaction value is another important factor that identified in [1]. A transaction value is the value of a service that participant paid for. This factor should be incorporated to evaluate the quality of feedback for a transaction [18]. The rational is that participants may choose transaction at a lower value of service as often as possible in order to submit ratings in specific period of time which has been identified as costly [25]. The behaviour and performance of online market participants' change over time therefore trustworthiness does not remain the same value. As Manchala [66] pointed out transactions conducted during a certain period of time can reflect a state of change in relation to trust. Thus, it is necessary to include time factor to degrade the value as trust value of sellers and buyers change overtime. Many approaches, however, assume that the behaviour of both sellers and buyers do not change over time and therefore do not take the time factor into account [39]. In most of the existing approaches, feedbacks suspected or found to be false are usually discarded. In our case, we keep them and evaluate them for later use in determining the trustworthiness of users.

The feedback verification mechanism takes the raw feedback and combines it with the information of participant's transaction history which is records in the transaction record component. A verifying scheme is used to determine if a feedback is genuine or suspicious. Suspicious ratings are maintained for further evaluation to determine the weight of the ratings. Also, both genuine and suspicious ratings have a trust score. Figure 4.2 shows a high level view of the feedback verifying strategy. The verifier is composed of a "history manager module" that manages the rating history for all users, a "feedback verification mechanism module" which is responsible for managing the feedback verification processes and a "feedback manager module" that is responsible for rating including both good and suspicious ratings. The following described and explain each of the components and the overall process of the proposed feedback verification mechanism that verifies the reliability of feedback.

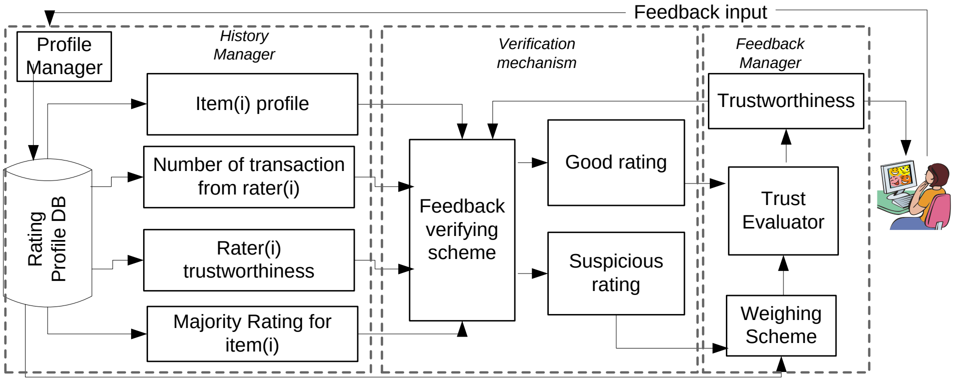


Figure 4.2: Feedback verification framework

Users submit a rating about a service/product after each transaction to the "Profile manager". The rating contains transaction information including the buyer ID, product ID, and seller ID, timestamp of the rating submits and the rating which is an integer value. This rating can be either a truthful value or a malicious value from the participant. The "Profile manager" manages the profile of all ratings received from users. Profile manager manages this information by using a rating profile database that stores all ratings information including the item profile (information of products), the number of transactions that the participant have done and the majority rating for the each item rated. The trust information of both the buyers and the sellers are also available from the rating profile database. All these information will be used by the feedback verifier to verify the credibility of ratings.

The feedback verifier does this by using its verifying scheme. It first combining the all transaction information including the buyer ID, product ID, and seller ID, timestamp of the rating submit and the rating value. To determine the suspicious rating from the genuine rating, the feedback verifier computes the rating using a verifying scheme. It first examines the majority of ratings from participants whose have high trust value within a timeframe, for example, a day or a week depending on the need of the system. All ratings within this timeframe fall within the set threshold and are considered good ratings because they satisfy the rules for rating credibility. If the credibility of the rating is high, it is considered as good rating otherwise it is group as suspicious ratings. The suspicious ratings are then calculated by the proposed weighing scheme. The feedback manager makes a decision as to how much weight should be given to the rating based on the information from the "transaction record" about past transactions of the participant. All weighted rating scores are then used by the trust evaluator to determine how trustworthy a participant is. This information is recorded and the trustworthiness of the buyers and sellers rating is updated. The detail of the verifying scheme is as discussed in the following section.

4.4 Feedback Verification Scheme

In our approach, we use k-mean data clustering to define the majority rating by grouping similar rating together [77], [109]. This algorithm assigns each object in the data set to the nearest cluster to create the clusters on all current reported ratings. The most densely populated cluster is then labelled as the majority cluster and the centroid of the majority cluster is taken as the majority rating. Also, we take into account the quality of rating included in the trust value of the participant based on his/her past behaviour, frequency (number of times) of rating submission and service/product value (price). The quality of rating is computed based on the majority ratings, trust value of participant, transaction frequency and transaction value. The goal is to verify suspicious ratings from all submitted ratings, before these ratings are accumulated and used to determine the credibility of sellers in the online eCommerce environment. Therefore, to determine the quality of a rating, a Trust Threshold is taken as a minimum value required depending on the sensitivity of the application, service requested or provided to establish trust relationship with any entity.

In the first stage, the ratings that fall on the majority cluster are combined with the three factors: trust value of participant, transaction frequency and transaction value. In this stage, ratings which are not in the majority cluster are ignored. The calculation of each of the parameter is used to determine the credibility of ratings. The trust value of participants can be extract from the rating profile database if the participant has established the most recent trust value. However, for participants who do not have trust value assigned to them, their trust value is calculate from their past transaction history. The calculations include time and rating value of transactions. Then the transaction value and the frequency of ratings submission are calculated. An adjustment scale factor is used in both parameter of transaction value and frequency value depending on the trustworthiness of participant. It has the effects on influencing the credibility of a rating. A participant with a higher level trust value, emphasis less weight the other two parameters. The approach is based on the assumption that low trust value participants are more likely to falsify ratings [30].

In the second stage, the three above credibility factors are combined to form a rating verification metric. The filtering mechanism employs this metric to determine the quality of a submitted rating. The result of the metric is act as a threshold. If the rating value and the result of this metric is the same, it is a good rating and is ready to use to evaluate a seller trust; otherwise it is a suspicious rating. In the third stage, all the suspicious ratings are given a value using a weighing metric, which includes a calculation of a rating variance from the value of the good rating. In this stage, the rating from either the majority cluster or away from the majority cluster is combined before the calculation. First, the variance of rating to the majority rating is calculated. Then the transaction value and the frequency of ratings submission are calculated. The weight of a suspicious rating is then given based on the rating weighing scheme. Table 4.1 provides the description of the symbols used in the rest of the chapter.

Table 4.1 Symbol and representation

Symbol	Description	Symbol	Description
r	Feedback rating	b	Buyer
M	Total feedback ratings for a given product /service	s	Seller
f_v	Rating frequency	$\mathfrak{M}$	Suspicious rating
∂	Weight given to a rating differences	W	Window size
β	Weight given to low value transaction rating	τ	Aging factor
λ	Weight given to rating frequency	p	product/service
$\aleph\vartheta$	Scale factor for rating submission interval	t	Time
t_i	Total number of submission of a service	t_v	Transaction value
$\mathbb{N}$	A scale factor for transaction value	v_i	Feedback value
$\mathbb{H}$	A scale factor for frequency	T_i	Trust Value
Δt	Difference between the current time and the recording time of the rating r_i	R	Ratings
Ω	Difference between a rating submitted by a buyer and the threshold set for a service	Cr_i	Credible rating

Let r_i be a rating submitted by a buyer (b_i) for a seller (s_i) for a product/service (p_i) at time (t_i). It is assumed that most of the ratings are submitted to a system at different points in time. Therefore, a system will receive M number of ratings $R = \{r_i(t_j), r_j(t_i), \dots, r_m(t_m)\} \mid i = 1, 2, \dots, M \mid$ for a given product. Similarly, $r_i(t_j)$ is a rating submitted by participant j at time i for a service (p_j)) and $r_m(t_i)$ is a rating submit by participant m at time i for service (p_m).

The ratings within a given time t_i are grouped using a window size W. This window size can be set to a day or a week depending on the needs of the system. The number of ratings in the window is not known in advance and it may vary over time. The window size should be considerably small so that any change in the behaviour of a given seller is minimal within each element of time. Also, a threshold value is used to differentiate ratings from the normal ratings.

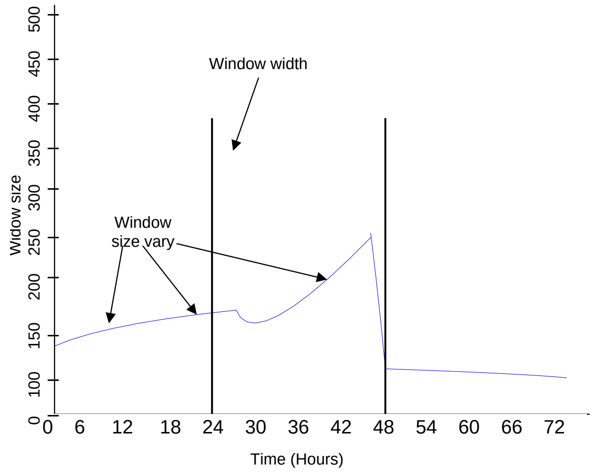


Figure 4.3(a) Vary window size

Figure 4.3(a) and figure 4.3(b) show examples of the window size that can be set at every 24 hours for a threshold of 0.8. The threshold is an expected value for the service. This means the ratings is evaluated daily and any rating below or above the threshold are suspicious ratings. In this example, the window size set has a total number of 4,550 ratings. All suspicious ratings become the input to the feedback manager, which determines the degree an individual rating can be trusted. A participant may rate the same service differently without any malicious intension. Thus, the quality of a rating may change in a number of ways depending on the factors mentioned earlier

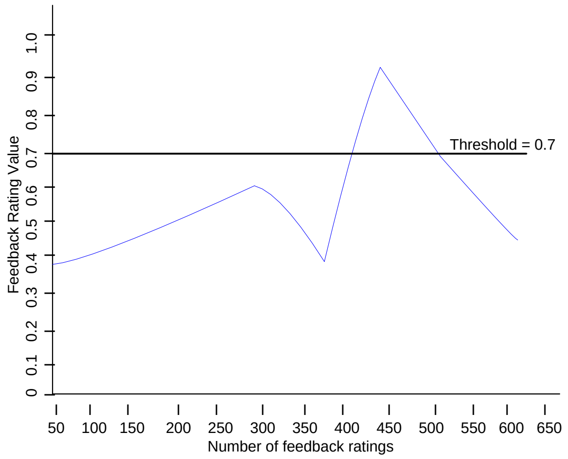


Figure 4.3(b) Set window size and threshold

The following Figure 4.4(a) shows an example of how the quality of rating is obtained from majority rating. All ratings received were calculated and the value of 0.9 has the highest number of the total ratings in which the majority ratings is 26 percent of the total number of ratings received. Figure 4.4b shows the parameters used to determine the quality of a rating. The quality of a rating is computed using the following formulation in section 4.4.1 which is based on the majority ratings.

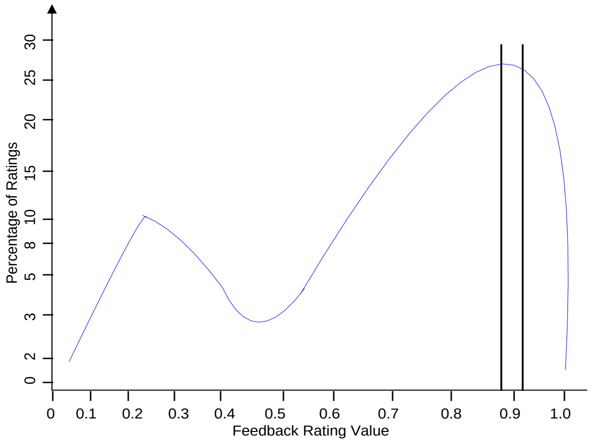


Figure 4.4a: Set majority rating

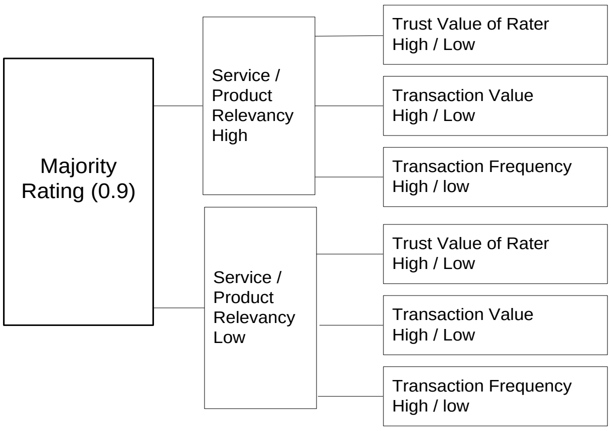

Majority Rating (0.9)
Service / Product Relevancy High
Service / Product Relevancy Low
Trust Value of Rater High / Low
Transaction Value High / Low
Transaction Frequency High / low
Trust Value of Rater High / Low
Transaction Value High / Low
Transaction Frequency High / low

Figure 4.4(b): Parameters used in determine ratings quality

4.4.1Computing Rating Credibility

Trust value of a seller is aggregated from ratings provided by buyers. Ratings received from buyers for a seller could be from many different services interacted. Therefore, the assessment of trust value of a seller is based on relevant ratings from the service required.

Aging factor. Similar to previous work [103], we included an aging factor to degrade the trust value of sellers' overtime. This can be seen from equation 4.1.The rating aging factor is scale according to the time of the rating received. Let $\Delta t \mid 0 \leq -\Delta t(r_i) \leq 1$ denotes the difference between the current time and the recording time of the ratingr_i. Let the parameter τ be the aging factor, which is mainly used to decide the level of emphasis given to the past level of trust of the buyer's when calculating the current trust value. Complete distrust is represented by 0 whereas 1 corresponds to full trust. Similar techniques are used to measure the trust value of a seller. The trust weight for a given rating is determined as shown below:

$$R_i = r_i . e^{\frac{-\Delta t(r_i)}{\tau}} \tag{4.1}$$

R_i is an indication of the weighted rating assigned by a given participant who has previously conducted business with the seller.

Trust value measurement. The trust value factor is measured by the ratings submitted for a similar of service. The trust value of a user is based on the average of the weighted transaction ratings of that service using aging factor. Equation 4.2 shows the calculation of trust value of a seller of service (i).

Let T_i denote the trust value where m is the total submission of weighted rating R_i for the seller i. T_i is computed as follow:

$$T_i = \frac{1}{m} \sum_{i=1}^{m} R_i \tag{4.2}$$

Transaction values measurement. A transaction value is the value of a service that a participant paid for. Equation 4.3 is used to measure the transaction value. The weight of the transaction value is measured by its proportion to the value of transactions. That is the differences between the average transaction value and the participant's total transaction value of a similar service. The larger the difference, the higher possibility that a participant is suspected to be malicious. A scale factor $\mathbb{N}$ (discussed in section 3.2) is used to adjust the transaction value.

Let the parameter t_v denotes the transaction value. It is computed based on the total transaction value (v) from participant (r_i) over the average transaction value of service (p_i) as follows:

$$t_v = \frac{\sum_{i=1}^{v} r_i}{\frac{1}{n}\sum_{i=1}^{n} p_i} . \mathbb{N} \quad (4.3)$$

Transaction Frequency measurement - Transaction frequency is the number of time that ratings are submitted to a seller by a participant comparing to ratings submitted by other participants during a set period of time. Equation 4.4 shows the measurement of the value of transaction frequency.

The parameter f_v denotes the value for frequency of ratings submission and is computed based on the total number of times (k) the ratings from participant's submission over the total number of ratings submission (n) for the service. Similar to equation 4.3, an adjustment factor scale $\mathbb{H}$ is used to indicate an adjustment value of that service. We compute the frequency of rating submission value (fv) as follows:

$$f_v = \frac{\sum_{i=1}^{k} v_i}{\sum_{x=1}^{n} t_x .} . \mathbb{H} \quad (4.4)$$

Where v_i is the ratingthe rating is value, and t_x denotes the total number of rating submission by that service.

Credibility of Rating Measurement - The above value of R_i T_i , t_v and f_v are releted to each other and are used to determine whether a rating. Equation 4.5 is used to compute the credibility of a rating in a set timeframe (between t_1 and t_2). A genuine rating (Cr_i) rating should have the equivalent value to the result; otherwise it is a suspicious rating. The quality of a rating is calculation as:

$$Cr_i = (r_i . \frac{T_i + f_v + t_v}{3}) \quad (4.5)$$

Thus, the result can be used as a trust threshold to compute credibility of the rest of ratings for a particular service in a set timeframe.

4.4.2 Weighing of Suspicious Ratings

(Cr_i) is used as a trust threshold for the following sections. A trust threshold is used for every rating according to the above-mentioned characteristics. Each of the ratings in a set timeframe was given a score from 0 to 1 according to the variance between the set thresholds. If a rating falls below the threshold, it is considered to be suspicious. As we discussed earlier, suspicious ratings are not discard, instead a weighing scale is used to weigh the suspicious ($\mathfrak{M}$) ratings. In the following, we explained how the weight is determined for suspicious ratings.

Once a rating is identified as suspicious, it is then placed in a suspicious group for further weighing. There are four weights used in the proposed weighing scheme which are associated with the following parameters: the different between the value of (Cr_i) and suspicious ratings ($\mathfrak{M}$) percentage of transaction value, feedback frequency and the suspicious rating value. The suspicious rating is then weighted according to the weight given to all the parameters. An aging scale is later used to scale the value of a suspicious rating. Each suspicious rating is scored between 0 and 1, with a higher value indicating higher suspicion towards a rating.

First, we show the individual weighing metric and later we show the weight metric given to a rating identified as suspicious.

Weighing differences between rating value - Let $\Omega t_i r_i$ be the difference between the rating submitted by a buyer and the threshold set for a service. γ is the scale factor set by the application that is used to decide how much of the majority vote is taken into account when calculating the significance of a rating, where $0 \leq \gamma \leq 1$, The rating ∂ associated with the majority vote is computed as folows(4.6):

$$\partial = \mathfrak{M}_{ri}.(e \frac{-(\Omega t_i r_i)}{\gamma}) | \; 0 \; \leq \Omega t_i r_i \; \leq 1 \; | \tag{4.6}$$

Thus, the higher the value ∂ is, the less weight a rating is given. Note that a rating submitted by a buyer is considered less value rating if the rating deviates from the threshold even though the rating falls within the majority votes.

Weighing Low Value Transactions - Ratings submitted by a seller/buyer within a specific time frame is calculated. The total ratings are clustered into individual groups based on the individual participant ID. The transaction value of each rating submitted is also identified. Let η be is the total transaction value submitted by a buyer, μ be the percentage of low value transaction and l_v is the set threshold. The weight of transaction value (β) is calculated as follows (4.7):

$$\beta = \frac{\mu}{\eta} - l_v \tag{4.7}$$

Weighing Feedback Frequency - Based on the timestamp of every rating submitted, an average time interval of ratings submitted for a seller is obtained during a specific time frame. A scale factor is then used to weigh any rating that is submitted at an abnormal rate of recurrence by a participant as follows (4.8):

$$\lambda = e^{-\aleph\vartheta} \; |0 \; \leq \aleph\vartheta \; \leq 1 \tag{4.8}$$

where ϑ is the difference between the average submission time interval of a buyer and the average submission time of buyers to a seller. A scale factor $\aleph$ is set by the application used to decide how much weight should be given based on the threshold.

Weighing Trust Value - The equation 4.1 and equation 4.2 are used to measure the trust value of a seller.

4.4.3 Weighing a Suspicious Rating

The weight of a suspicious rating is based on the four related factors ∂, β, λ and T are calculated as follows:

$$\mathfrak{M}_{\mathrm{ri}} = \frac{\partial w_1 + \beta w_2 + \lambda w_3 + T w_4}{w_1 + w_2 + w_3 + w_4} \tag{4.9}$$

where w_1 the percentage of participation, $w_2$be the percentage of low level transactions, w_3 be the frequency of submissions and w_4 be the trust value of an individual rating. These weighted ratings can be included in computing trust value of a seller when there have not enough ratings to evaluate trust value of a seller.

4.5 Performance analysis

The first set of experiments testing the performance of credibility of ratings with various setting of parameters. There are three group of testing in this set of experiments. The result of original ratings is compare with a ratings group with high quality sellers (different attributes are pre-defined with majority rating of 0.8). The next group performs with consistently low quality sellers (different attributes are pre-defined with majority rating of 0.3). The third group performs with high values seller with an aging scale.

The second set of experiments set out to demonstrate how the volatility of the majority of ratings can be achieved in a number of ways when compared with an average of ratings. The results indicate that when there is an increase in malicious ratings within a particular time frame, these could increase the likelihood a rating chance will become part of the majority ratings. The third set of experiments was to study the impact of the four different weighing scales on the parameters we used. As stated earlier, in eCommerce environments, it is impossible to totally differentiate the unfair rating amongst all other ratings. The proposed method aims to minimize the influence of malicious ratings in trust evaluation. Our proposed weighing metric calculates the value of suspicious ratings.

We will show and discuss the simulation results in the following section. We then compare the proposed model with the standard reputation-based system. In particular, we focused on the stability of both models when the number of untrustworthy seller increasingly varied in the system. We created 100 sellers selling the same product. Among them are those with a high trust value (trustworthy) and others with a low trust value (untrustworthy). Participants were randomly chosen for the assessment. In the simulation, the participant trustworthiness is generated randomly for each buyer and seller in the range of [0, 1].

4.6 Simulation Result and Discussion

The trust value is calculated using the credibility filtering function in equation 5 and all three parameters are set as high values. The result is compared with the original seller's trust value (where trust value is the accumulation of majority ratings). The results are shown in Figure 4.5 and Figure 4.6. When credibility filtering function is applied for a high trust value seller, the seller performs consistently with high quality values comparing with the majority ratings. The assessed credibility is shown for two main scenarios. In this scenario, the majority of participants have high trust value, with higher value of transactions. Result shows the credibility of ratings is very close to the original majority rating since the trust value and the transaction value of participant is high. Both majority rating and result shows the rating credibility degrading after a period of time as the aging scale is applied to the Equation 4.5 and Equation 4.9.

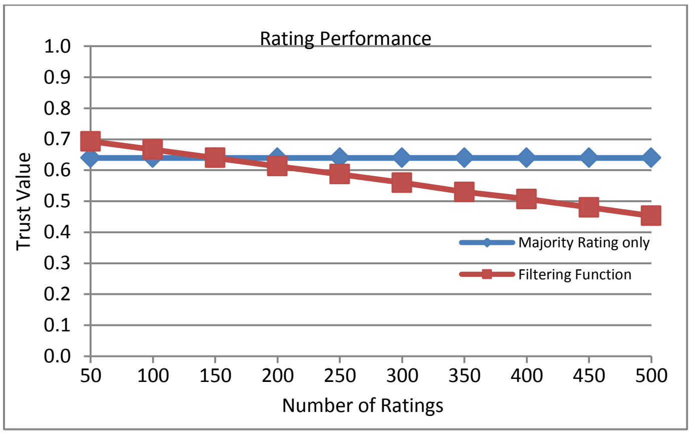


Figure 4.5 Comparison of rating performance when trust value and the transaction value is high

In the second scenario, malicious participants are more than the honest participants. The majority ratings are low value. Figure 4.6 shows the result rating credibility is very low compares with the original ratings. Since low values are chosen, rating credibility suffers low decrement in the case of dishonest ratings from malicious participants. However, in this scenario, the large number of malicious participants directly affects the majority rating and hence the final assessed reputation. Therefore, the assessed credibility is not close to the performance of using majority ratings. In this case, the majority rating is given a false trust value of a seller. The result also shown the aging scale is applied to the testing result but not to the majority ratings performance. The results indicated that applying the credibility filtering function to evaluate the trust value of sellers is giving a more accurate performance.

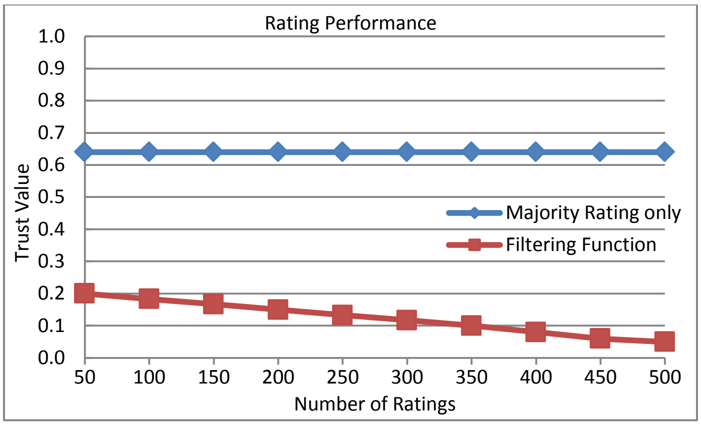


Figure 4.6 Comparison of rating performance majority ratings are low value

4.6.1 Weighing Trust Value

For example, 1,000 ratings that were received for a product p_1 sold by a given seller. These ratings were received between the timeframe periods of T_1 to T_{10}. Accuracy is a result represented by 0 whereas 1 corresponds to the total incorrect. In this example, a seller has a trust value of 1 (total trust). When 10 percent of malicious ratings are inserted among these ratings, the true rating value starts to degrade. The result shows that the increase of malicious participants participating in the community leads to an imprecise majority method. When 100 percent of malicious participants exist within a set time frame, a seller's trust value could fall from 1 (total trust) to 0 (totally untrustworthy), with the accuracy also 0. Or it could be manipulated from total distrust (0) to full trust (1). These results indicate that when the rating is submitted by a participant within a certain time period, their chances of receiving majority ratings increase. Thus, a majority rating is not always representative of a true rating and the result could be misleading.

Figure 4.7 shows the results from simulations of the two models. It shows the comparison of both models in terms of the error rate when the number of malicious of participants increase. The error rate of our proposed model is rather consistent when compared with the model used to determine majority ratings. The majority model (BRS) is very sensitive because the predictions of future behavior depend entirely on the majority ratings submitted by the participants. In our experiment, we took into account the four parameters discussed in section 3.

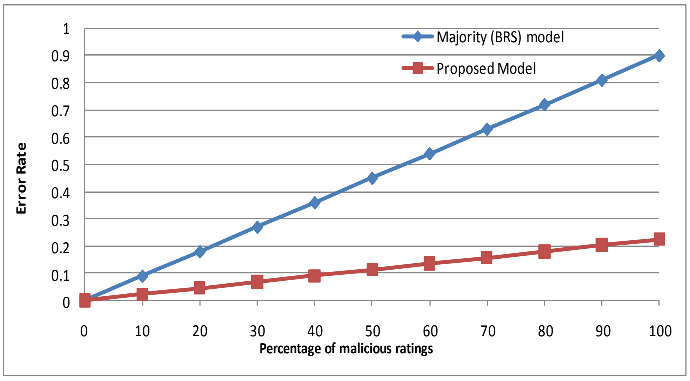


Figure 4.7: Comparison of Two Models

In e-Commerce, a participant can register as many identities as they like. It is impossible to know the actual identity of a person or that b_1 is actually b_2. Most trust models suggest it is safe to have business transactions with those who have higher trust values [25]. Although trust value is one important factor, we cannot assume that all trustworthy sellers or buyers provide honest feedback. It is quite often a seller who has been in the e-market business for a long period of time and established a high level of trust who can decide to cheat any given time. The majority models (BRS) could not predict changes in the behavior of participants behavior and could not indicate the malicious ratings. On the other hand, our proposed model not only considers the majority ratings but also the transaction properties discussed in section 4, which are the value of ∂, β λ and φ. These values is introduce to produce more stable results as these factors act as a constant value and are applied into the equation. Thus, one bad transaction is not likely to reduce trust of proportion to the number of successful transaction.

4.7 Comparative Analysis

In this subsection, we compare the proposed model with the standard model (BRS) using majority votes. In particular, we focus on the stability of both models when the number of untrustworthy participants varied greatly in the system. Figures 4.8 (a), figure 4.8(b) and figure 4.8(c) show the experiments results when the values of various parameters changed. The results indicate the proposed weighing metric produces a stable result even though there were increases. Normally, the results using majority metric remain rigid. From the experiments result, we believe that trustworthiness of participant and seller, age of rating and frequency of rating are important parameters that should be considered in the design of a rating verifying scheme. In order to evaluate the performance of our model in different scales, we tested the three parameters β, λ and φ with different value but were given equal weighing scales. First, the three parameters were tested with maximum value of 1, then with least value of 0.1. and lastly, one of the parameter β is set as maximum value of 1 and the other two parameter λ and φ 0.1. The results are shown in figure 4.8(a), 4.8(b) and 4.8(c) respectively.

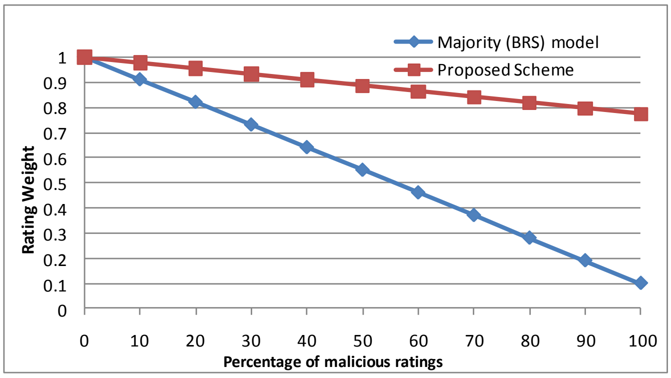


Figure 4.8(a) Weighted result when β =1

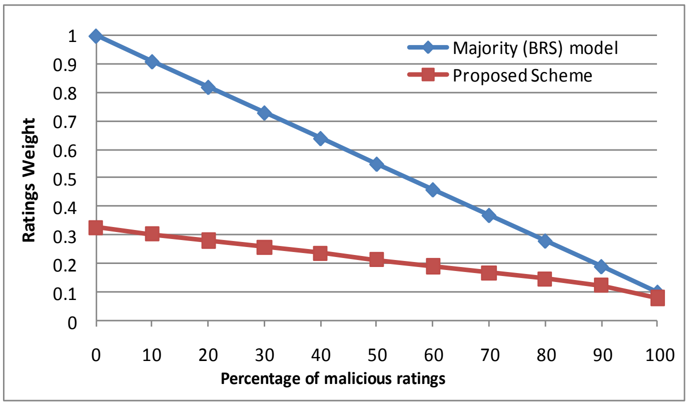


Figure 4.8(b) Weighted result when β =0.1

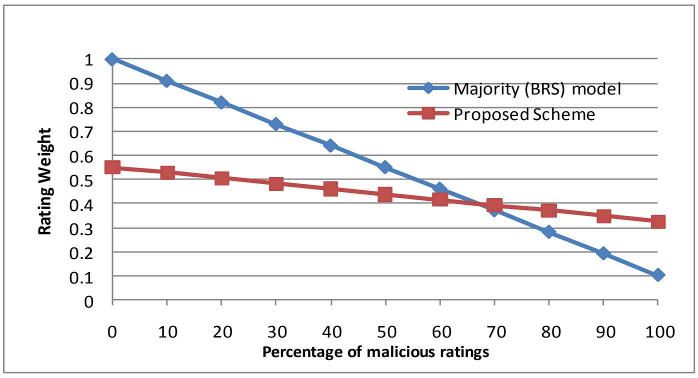


Figure 4.8(c) Weighted result when φ=0.1

Figure 4.8: Weighted result when equal weight given and β =1, λ=1, φ=1 (a), β =0.1, λ=0.1, φ=0.1(b), β =1, λ=0.1, φ=0.1 (c)

In Figure 4.8(a), we can observe that as the percentage of malicious ratings increases, both models show the decrease in the value of ratings. While our model decline slightly but it is very close to the original value. However, the standard majority model departs away from the original value. We again observe that the result shown in Figure 4.8(b) is similar to the results shown in Figure 4.8(a). The result in Figure 4.8(c) shows that our model remains stable although the maximum and minimum values of the parameters are used. Therefore, when the majority of participants provide ratings, the rating in question will not have a significant influence on the trust value in the proposed model. Furthermore, the proposed model is able to produce results even when a lower number of ratings are received. Trust models that use majority metrics are unable to produce results when ratings are low.

We performed a simulation study using 5000 samples. To validate the accuracy of our results, we run the simulation with a number of different set of random numbers which is generated mathematically. We have run the simulation 100 times for each of the alternative factors. For each run we have used different random numbers and obtained the output figures. For all samples, we estimated the standard deviation of samples and the true standard deviation. The results shows the confident levels we get are 95%. Therefore, we can say we are 95% confident that the accuracy of the simulation results.

4.8 Chapter Summary

In this paper, we have discussed the properties and challenges of trading in eCommerce trust management systems. We showed that exiting trust management systems are fallible to strategic manipulation of the feedback attacks and proposed an algorithm to detect suspicious ratings and exclude it from trust calculation in order to improve the reliability of the trust management system. The viability of the proposed approach is studied experimentally and the results of various simulation experiments show that the proposed approach can be highly effective in identifying falsified feedbacks. We also compared the proposed model against the majority vote model. The result shows that our model is more stable than the majority-based model.

Chapter 5

Risk-based Online Engagement Decision Making

This chapter presents an approach for determining risks involving the exchange of goods and services online between two or more parties. In the presence of biased online feedback ratings, the proposed approach enables potential buyers to determine the risk level of a product before committing to proceed with the transaction. This is useful to online buyers as it allows them to be aware of the risk level and subsequently take the appropriate actions to minimize potential risks before engaging in risky businesses. Results of various simulation experiments show that the proposed multi-attribute trust management system can be highly effective in identifying risky transaction in electronic market places.

5.1 Introduction

The focus of this chapter is on augmenting the potential online buyers' decision making process by exposing the potential risk levels of a given transaction to them. This trust model differs from the exiting trust management systems in that we attempt to connect risk and trust management systems in an e-market environment. This is useful to online buyers as it allows them to be aware of the risk level and subsequently take the appropriate actions to minimize potential risks before engaging in risky businesses. Predicting risks is possible by looking at the information collected in the previous steps. An idea about the type of risks, where, when and how they occur, makes the forecast of impending risks more accurate. According to Amland [4], information about history and knowledge of previously identified risk helps to predict risks correctly and thus increases customer confidence.

The trust model offers a comprehensive approach by incorporates important properties of the product or services as well as the trustworthiness of the service providers in assessing online transaction risk in order to enhance the mechanism of buying decision. Moreover, this approach quantifies three real-life parameters in order to be used efficiently in transaction risk evaluation. It takes into account of warranty as an element of risk reduction factor. It is also independent of transaction history. As a buyer may make complaint after several months of receiving the goods, transaction history based systems fail to capture such cases. Also, as sellers' behavior is difficult to predict, we think the property of a product to be purchased should be considered in every product or services. This new multi-attribute risk technique that can inform potential buyers the risk level associated with a given product. This helps the buyers to make informed decision before proceeding with the purchase of the product.

5.2 Risk-Driven Trust Management

We discuss a multi-attribute risk management system which takes into account properties of the products or services such as price, quality and the reliability as well as the trustworthiness of the service providers to compute the risk levels.

5.2.1 Highlight of the Framework

We believe that trust, product price and quality are some of the important parameters that should be considered in the design of trust management systems. The purchase of a high ticket items requires a great deal of information as the risks involved in such a purchase are substantial [44]. Trust is relevant to risky situations [4] and helps deal with uncertainty[6]. As risk is a function of the cost of goods and services [61], the price of the product generally has direct influence on the level of trust. Although, many people shop on price, but the willingness of a consumer to pay a high price depends on his/her being convinced about the quality of a product [43]. Therefore, trust, price and quality of the product are three important and inter-related variables that need to be taken into account in the design and development of a trust management system to help online buyer’s concern to make a purchase decision.

In e-Commerce, like any business transaction, at least two sources of risk and two types of claims can be associated with a given product. The first risk is that the product does not meet the specified (promised by the service provider) properties, during the specified period of its life. The second risk is that the product does not meet the expectations of the buyer. Precise assessment of these risks is critical for the success in e-Commerce. Warranty addresses this kind of risks and helps online transaction to reduce perceived risk [66]. According to marketing signal theory, product warranty is a tool that serves as a signal to provide information about the quality and reliability of the product or service [5]. Warranty can also represent how fragile (delicate) or robust a product is especially when the knowledge of product quality is difficult to obtain by consumers. The longer the warranty period indicates the better quality of a product [43]. Due to the warranty costs in the event of product failure, the manufacturer will need to ensure high product quality if an extensive warranty coverage is offered. On the other hand, a poor quality product with high failure rate will not be able to afford extensive warranty coverage. Many online retailers sell warranted goods and research suggests that people felt comfortable buying online using eCommerce website if they see product warranty on the website [61]. For example, a search of the eBay site using the word warranty returns 16,072 matches. Individual service providers usually list the terms of their warranties, if warranties are on offer, or if they are transferrable from the original buyer to the next owner. Warranties supplied by manufacturers or service providers help to limit risks, the loss will be small when the expectations are not fulfilled since it assure by the warranty [73], [81] and [83]. As a result, the warranty of a product is able to create trust even under the overall condition of distrust.

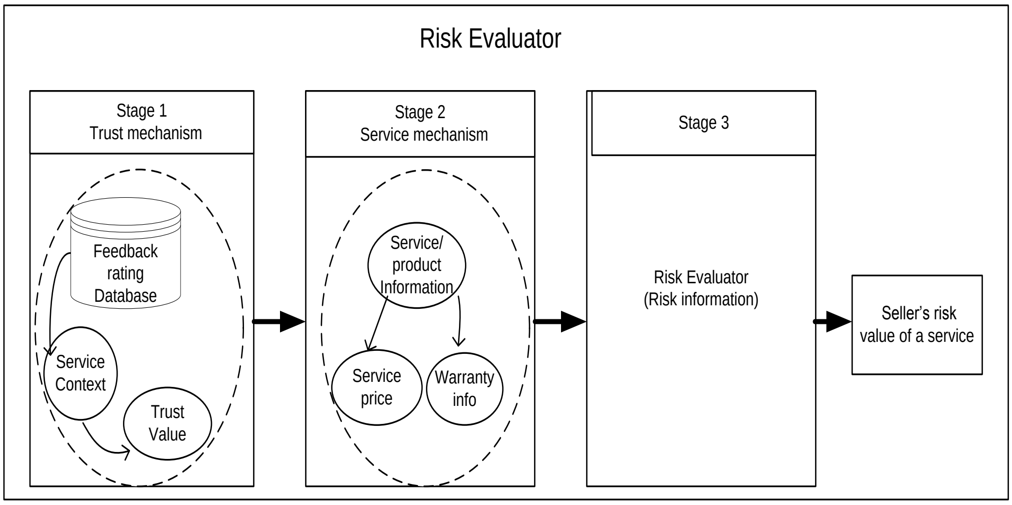


Figure 5.1: The process of risk evaluation

The above Figure 5.1 shows the simplified view of the overall modules of the risk evaluator framework. The risk evaluator is divided into three modules. There are a trust mechanism, a service mechanism and a risk mechanism. The trust mechanism manages trust value of a sellers based on feedback ratings received from buyers of service transactions. The service mechanism manages service information such as service id, service price (cost), service warranty length and its type. The risk mechanism is responsible for calculates and manages the information of transaction risk on a service of a seller.

In the first stage, the trust value of users is calculated. To calculate the trust value of users, the trust mechanism extracts the past transaction feedback ratings from the feedback profile database. These feedback ratings are obtained with the application of filtering mechanism. There have been filtered employs a few schemes of clustering filtering methods using similarities among the ratings. We applied the filtering method used in the previous chapter four. The trust value is then calculated based on the transaction rating, the relevancy of service requested and the time ratings being submitted.

In stage two, the service cost and the warranty cost of the service is calculated by the service mechanism. A service profile database keeps all information of services and warranty information of the feedback ratings of past transactions. The service mechanism obtains the service information from the service profile database. The service cost is the price or the value of the past transaction for the feedback rating. The value of service cost is calculated according to the size of the unit cost. The value of warranty is calculated according to the length and type of warranty of that service.

In stage three, the risk evaluator is responsible of computes individual risk value of a transaction service to a seller. When there is a request from a user for transaction risk information about a seller on a service, risk evaluator obtained all necessary information associate to the seller from trust mechanism and service mechanism. It first calculates the risk value on trust value of a seller, risk on service value and the warranty value before the overall risk of a transaction of a seller is calculated.

5.3 Risk Formulation

In this section, we present our risk formulation. Instead of considering all parameters equally, each parameter is weighted separately so that applications may customize different value for each parameter as needed.

5.3.1 Computing Trust Value Risk

Trust can be used to measure our confidence that a service provider in an eCommerce environment behaves as expected. However, due to the dynamic nature of trust, the value of trust at the beginning and at the end of a time slot will not be the same. In our model, trust value is weighted according to the freshness of the feedback ratings. We assuming that the feedback rating received is more accurate if it is relevant to the product of the potential transaction [90] and [108]. Therefore, the feedback rating is based on the relevancy and the time difference similar to [66]. This is because transactions conducted during a certain period of time could reflect a change of trust state [66]. The feedback ratings for the service provider are grouped into two subsets as relevant and irrelevant. This allows us to select the right subset of ratings for trust evaluation. In other words, we obtain feedback rating from the relevant group for calculating the trust value. However, when no relevant ratings are found, we used the other group of feedback ratings that is not relevant to the service.

In order to determine trust as a prediction of the future behavior, it is possible to specify, that the latest experiences ought to weigh more than the older experiences. The rational for this is that the quality of trustees is not necessarily fixed but may change over time, for example due to gathered experience in a certain field.

Let r_i be a feedback rating submitted by a buyer b_n after a successful transaction with a service provider $\mathrm{s_j}$ on a product $\mathrm{p^i_{s_j}}$. The cumulative feedback rating for the service provider is computed as follows:

$$\mathrm{F^n_{p^i_{s_j}}} = \mathrm{r.\, e}^{\frac{-\Delta\mathrm{t}(\mathrm{r_i})}{\lambda}} \,|\mathrm{F^n_{p^i_{s_j}}} \in [0,1] \qquad (5.1)$$

In Eq. 1.1, $\Delta t | 0 \leq -\Delta t(\mathrm{r_i}) \leq 1$ denotes the difference between the current time and the time when the rating $\mathrm{r_i}$ is recorded. The parameter $\lambda | 0 \leq \lambda \leq 1$ is the aging factor mainly used to decide how much previous history of the service providers trust level should be taken into the account when calculating the current trust value. For example, a user could decide that a feedback rating obtained 10 weeks earlier to contribute only half the effect of a new rating obtained today. The metric used for the trust measure in our proposed trust model is a real number in the interval of [0, 1]. Complete distrust is represented by 0 whereas 1 corresponds to full trust.

Let $\mathrm{T_{p^i_{s_j}}}$ denote the trust value of the service providers in the online market. Thus, $\mathrm{F^n_{p^i_{s_j}}}$ is an indication of the weighted rating feedback assigned by buyers who have previously conducted business with the service provider s_j

$$\mathrm{T_{p^i_{s_j}}} = \frac{1}{\mathrm{m}} \cdot \sum \frac{\mathrm{m}}{\mathrm{n=1}} \,|\mathrm{F^n_{p^i_{s_j}}} \in [0,1] \qquad (5.2)$$

where m is the total submission of weighted rating and $n \in [1, m]$. Thus, it is clear that the measuring of the trust value $\mathrm{T_{p^i_{s_j}}}$ is dependence on the freshness of the feedback ratings which can be adjusted according to the desire of the application.

Thus, the risk $\mathrm{D}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}}$ on trust value $\mathrm{T}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}}$ of the product $p_{s_j}^{i}$ is given as follows:

$$\mathrm{D}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}} = 1 - \mathrm{T}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}} \tag{5.3}$$

5.3.2 Computing Service Cost

Transaction price is scaled according to the size of the unit cost. As risk is a function of the cost of goods and services [66], the price of the product generally has direct influence on the level of trust. In general, consumers are more cautious when buying a product at higher price compared to a cheaper product.

Let β_i be the price of a given product $\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}$ sold by a given service provider s_j and α is the scale factor of the product cost. The risk associated with the given product price, $\mathrm{A}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}}$ is computed as follows Eq 5.4:

$$\mathrm{A}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}} = 1 - e^{-\alpha\beta_i} \mid 0 \leq -\alpha\beta_i \leq 1 \tag{5.4}$$

Eq. 1.3 allows users to adjust the risk level based on the amount of the product. For example, users can set the risk level to 1.0 when the price of the product exceeds $10K.

5.3.3 Computing Warranty Value

Warranty value is weighted separately according to the length and the type. The willingness of a consumer to pay a high price depends on shoppers being convinced about the quality of a product [43]. In general, online shoppers demand assurance that the purchased product will perform satisfactorily over its expected life. As a result, many consumers are known to have a higher tendency to buy a product that comes with a warranty program [69]. Warranties may reduce perceived performance risk by providing against product defects and premature malfunction of the product during the time that the warranty is in force. Financial risk may be reduced by a warranty protecting consumer against a large repair bill or having to replace the product during the warrant period. Thus warranties play a vitally important role in providing the assurance to the online buyers. Because online shoppers order goods without being able to handle or test them first, the product warranty offered by retailers is likely to help enhance in buyers trust in respect to the products quality [43] and [69].

Let wl and wt be the warranty length and the type of warranty coverage of a product $\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}$ respectively. The purpose of measuring product warranty is to obtain the appropriate warranty value $\mathrm{W}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}}$ which for a given product $\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}$. The risk on product warranty $\mathrm{W}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}}$ is measured as follow (5.5):

$$\mathrm{W}_{\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}}} = 1 - \ \mathrm{wl}\ \mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}} + \ \mathrm{wt}\,\mathrm{p}_{\mathrm{s}_\mathrm{j}}^{\mathrm{i}} \tag{5.5}$$

Warranty length defines the duration of the warranty period while warranty type is the warranty coverage type: (A) product parts only, (B) product parts and service charge only or (C) parts, service charge and other compensation, such as extended warranty duration, gift voucher, replacement of new product, etc. Different weight of the warranty risk is given according to the different warranty's coverage type, where (A) > (B) > (C).

The information shown in Table 5.1 is the measurement of the warranty length and warranty type. To simplify the calculation, the percentage obtained in Table 5.1 is divided by 100. To decide the percentage of the warranty length and warranty type, an average coverage type of a product is taken into account. For instance, when we buy a laptop, the maximum warranty coverage will be three years.

Table 5.1: Product warranty and weight

Product	***wl***	***wt***	***Total Warranty***	***(Weight)***
1	*1*	*C =1*	*0.865*	*0.135*
2	*0.66*	*C=1*	*0.810*	*0.190*
3	*0.33*	*C=1*	*0.736*	*0.264*
4	*1*	*B=0.66*	*0.810*	*0.190*
5	*0.66*	*B=0.66*	*0.736*	*0.264*
6	*0.33*	*B=0.66*	*0.628*	*0.372*
7	*1*	*A=0.33*	*0.736*	*0.264*
8	*0.66*	*A=0.33*	*0.628*	*0.372*
9	*0.33*	*A=0.33*	*0.484*	*0.516*

According to the Consumer reports [21], the average warranty coverage of electronics and electrical appliances is approximately three year. Nevertheless, the weighing scale can be adjusted according to the service average life span. Note that we do not take into account extended warranty coverage. In this example, since three years is the average warranty coverage for a laptop, any warranty duration offered that is three years (36 months) or more will receive the minimum risk value 1/3. Warranty duration of one year will have the maximum risk value of 1, and two year duration but less than three years will have the two third of the maximum rate. Similarly, to obtain the percentage of warranty type, we set C = 1/3, B = 2/3 and A has the maximum risk value of 1. From this explanation, the item 1 have both warranty duration and warranty type as maximum of 1, and weight given to the item indicates a value of 0.135 compared with the item 9 of 0.516 which has the lowest total warranty. The information also shows that an item has maximum warranty duration of 1 and it does not necessarily have a lower risk. From the above information, it is clear that the weight of warranty is depending on both duration and coverage type.

5.3.4 Computing Transaction Risk

The transaction risk is computed based on the trust, product price and warranty parameters. The goal is to produce a risk indication of a product for potential buyers in the present of unknown online eCommerce environment. The overall risk level of a given transaction is computed as follows:

$$R = w_1 \ D_{p^i_{s_j}} + w_2 \, W_{p^i_{s_j}} + \ w_3 A_{p^i_{s_j}} \ |(w_1 + w_2 + w_3) \tag{5.6}$$

The highest value of the risk indicates the highest risk of the transaction. The parameters $D_{p^i_{s_j}}$, $W_{p^i_{s_j}}$ and $A_{p^i_{s_j}}$ represent the risk of trust level, the risks to warranty and the price levels respectively. The parameters w_1, w_2 and w_3 are used to scale the risk to trust level, the risks to warranty and the price levels. The purpose of differently weighting $D_{p^i_{s_j}}$, $W_{p^i_{s_j}}$ *and* $A_{p^i_{s_j}}$ is to have the flexibility and improve risk indication levels when there is no feedback rating for new service providers and when the feedback rating are irrelevant to the product.

5.4 Performance Analysis

To verify the effectiveness of the proposed trust model, we have carried out analysis of the risk-based trust management system using simulation. We also compared the proposed scheme with the reputation-based systems commonly used in systems such as eBay. In this section, we discuss the simulation setup and the results of the experiments.

We tested the performance of the proposed model with simulations in different eCommerce scenarios. Although it is not possible to exhaust all potential scenarios types, testing the protocol with a variety of scenarios gives an idea on the effectiveness of the proposed trust management system. In the simulation, the risk of trust value, $D_{p^i_{s_j}}$ is generated randomly for each provider in the range of [0, 1]. We used a 100 service providers selling the same product. Among them there are some with high trust value (trustworthy) and some with low trust value (untrustworthy). Participants are randomly chosen for the assessment. Average results of 100 interactions are simulated for assessing the risk value. We carried out several experiments. The first set of the experiments is to study the impact of the three different weighing scales we used. The weighing scale of feedback rating is conducted using different time length and different scale factor in the range of 0.1, 0.5, 0.7 and 1.0. For the service cost, we used \$0.1K to \$10K. A warranty length of 3 years is set as the maximum with any service that are equal or more than 3 years will have the minimum risk value.

The second set of the experiments is to compare the proposed model with standard reputation-based system. One well-known such system is the rating scheme used by the eBay online auction site. Reputation-based systems are used to establish trust in e-market places where transacting parties with no prior knowledge of each other use the feedback from the participants to assess the trustworthiness of the service providers in the e-market place. In particular, we focus on the stability of both models when the number of untrustworthy service providers increasingly varies in the system. Another experiment is carried out to study cases such as when the service providers are new in the market.

5.5 Simulation Result and Discussion

5.5.1 Impact of Weighing Scales

In order to determine trust as a prediction of the future behavior, it is possible to specify, that the latest experiences ought to weigh more than older experiences. The rational for this is that the quality of trustees is not necessarily fixed but may change over time. The parameter $\lambda \mid 0 \leq \lambda \leq 1$is the aging factor mainly used to decide how much previous history of the service providers trust level should be taken into the account when calculating the current trust value. For example, a user could decide that a feedback rating obtained 10 weeks earlier to contribute only half the effect of a new rating obtained today. That is the newest rating should have the maximum weight of 1 and any rating of 10 weeks and older should have the weight of 0.5.

Figure 5.2 shows the impact of the aging factor on the selection of the feedbacks. The aging factor in the interval of [0, 1] determines the ratio of a new experience to previous experiences in the update computation.

The result demonstrates that the recent feedbacks weigh more than older feedbacks. Proposed time factor is gives not only higher values to the most recent ratings, it also gives higher values to the higher λ. The means that whilst the feedback ratings have low value, it still places more weight on its feedback ratings. Likewise, the higher feedback ratings may not necessary have higher value as this rating is out dated. The performance shows that time is the direct influenced the weight given to the feedback ratings. Thus, the usefulness of feedback ratings is depending on when the feedback rating is received. In other words, the ratings value may fall below a predefined threshold over a period of time.

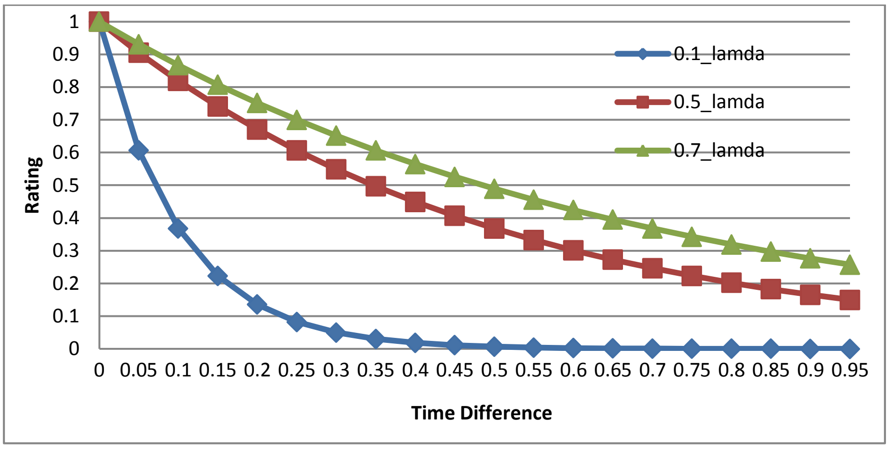


Figure 5.2: Measure of feedback rating over time

Even with the above mentioned aging technique in place, not every ratings submission that receives from buyers to seller is useful for trust evaluation. We proposed that weighing scale is applied to feedback ratings according to the transaction price. The below Table 5.2 shows the result of the different weights obtained from the product price when $100K and $l0K is set as maximum respectively. In both cases (i.e., $100K and $10K), the product price is set to $5K and the weight is set to 0.05 and 1 respectively. Then the weighted values $A_{p^i_{s_j}}$ of product cost $p^i_{s_j}$ are 0.0488 and 0.632 respectively.

Table 5.2: Scale of service cost

Product	*Cost β*	*(1) α*	*value*	*(2) α*	*Value*
1	*10-99*	*0.00001*	*0.0001*	*0.001*	*0.01*
2	*100-499*	*0.00001*	*0.001*	*0.001*	*0.1*
3	*500-999*	*0.00001*	*0.01*	*0.001*	*1*
4	*1k -4999*	*0.00001*	*0.1*	*0.001*	*1*
5	*5k -9999*	*0.00001*	*0.5*	*0.001*	*1*
6	*≥ 10k*	*0.00001*	*1*	*0.001*	*1*

We can observe form Figure 5.3 that when product/service cost increases the weight of risk is also increases. This shows that the proposed weighting scale is dependent on the size of the product cost. The weighing scale of individual feedback ratings is similar to the previous aging scale. Therefore, the usefulness of a rating is required to know the cost of the product/service for that rating.

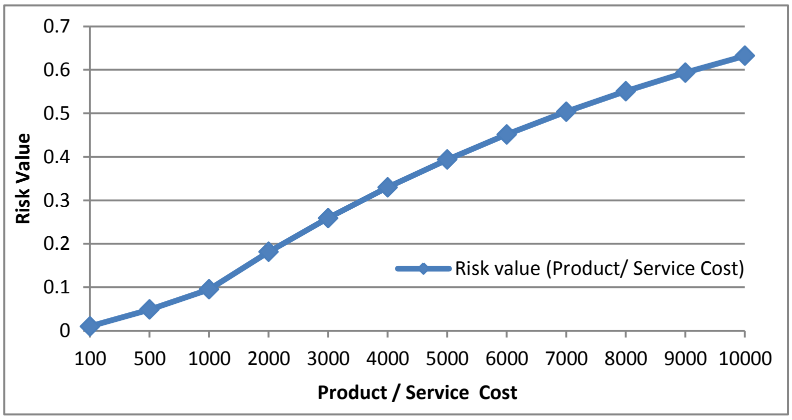


Figure 5.3: Measure of risk value against service cost

5.5.2 Comparative Analysis

We compared the proposed model with the standard reputation-based system. In particular, we focus on the stability of both models when the number of untrustworthy service providers increasingly varies in the system. We created 100 service providers that are in the online market selling the same product. Among them there are some with high trust value (trustworthy) and some with low trust value (untrustworthy). All one hundred of service providers participate on the assign product. Participants are randomly chosen for the assessment.

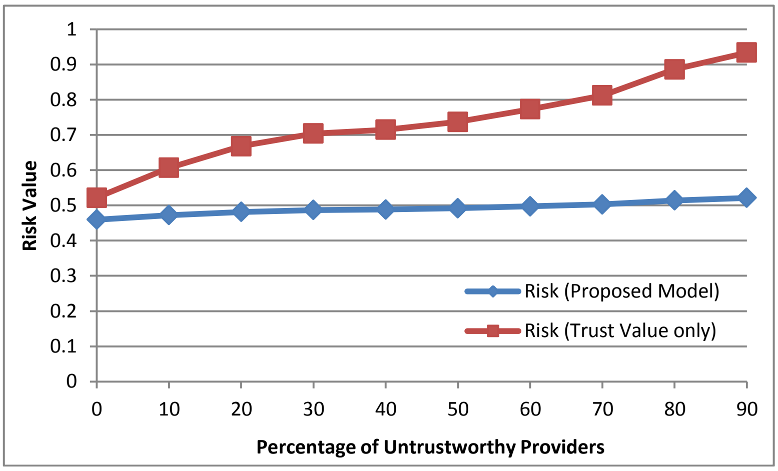


Figure 5.4: Risk comparison

Figure 5.4 shows the result of the simulations of the two models. It shows the comparison of both models in terms of the total risk indication when service providers are randomly chosen. The risk indication of our proposed model is rather consistent. The trust - value only model is very sensitive. This is because the trust value only model predicts the future behavior depends on the past behavior of service providers. It totally depends on the trust value of service providers, and did not take into account of the service information when assessing the risk value.

When buying in the open electronics market there are both trustworthy and untrustworthy service providers. Thus, buyers are more likely to conduct business with the service providers with a higher trust value. However, when service providers with high trust level change their behavior, most trust models could not correctly indicates the transaction risk when a potential buyer needs it. For example, a service provider that has been in the e-market business for a while can build up his trustworthiness and at a sometime can decide to cheat. The reputation-based system could not predict the change in the service provider and will indicate to the potential buyers that the risk of the transaction is minimal. On the other hand, the proposed model considers, in addition to the trust value of service providers, product properties namely the price and warranty as well. Thus, when the trust level of the service providers changes their behavior, the risk indication will not have much influence in the proposed trust management system.

Figure 5.5 - Figure 5.9 show the results of experiments when the values of the various parameters varied. The proposed model is able to indicate the risk value of a potential transaction.

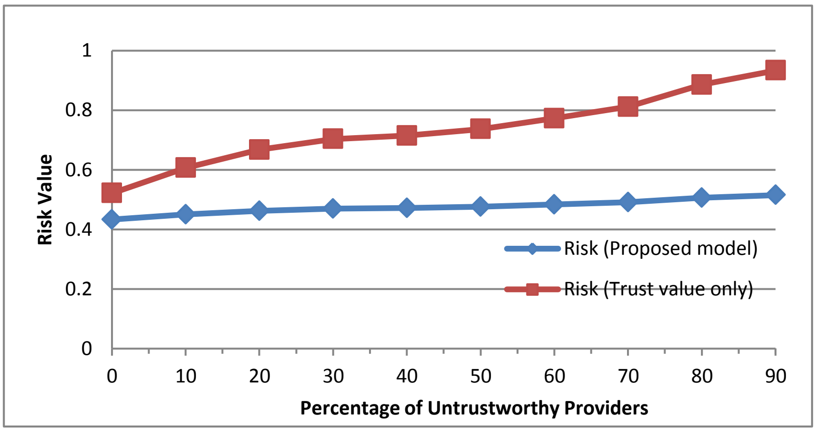


Figure 5.5: Risk result when weighted service cost =1, warranty =1 and trust value = Random

Figure 5.5 shows the results of risk value when trust value is relevant to the potential transaction. However, the value of product cost and the warranty are both set as constant to the highest level of 1. We can see that the risk values computed by both models show an increase when the percentage of malicious or untrustworthy service providers increases. The proposed model however performs fairly consistent with a slight increase as the percentage of the untrustworthy service providers' increases.

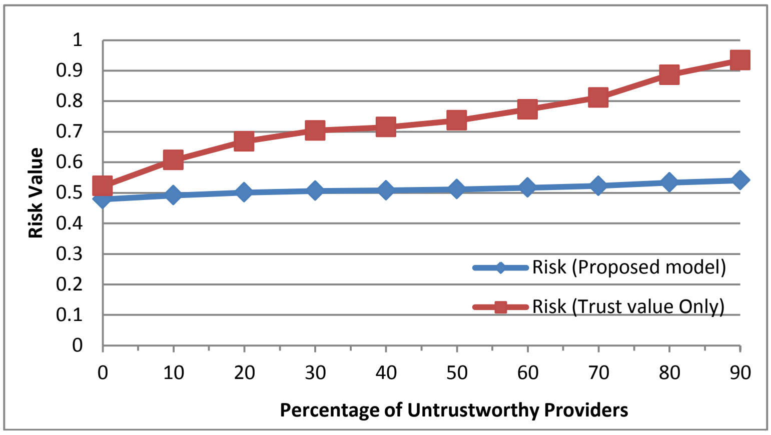


Figure 5.6: Risk result when weighted service cost=0.1, warranty =1 and trust value = Not relevant

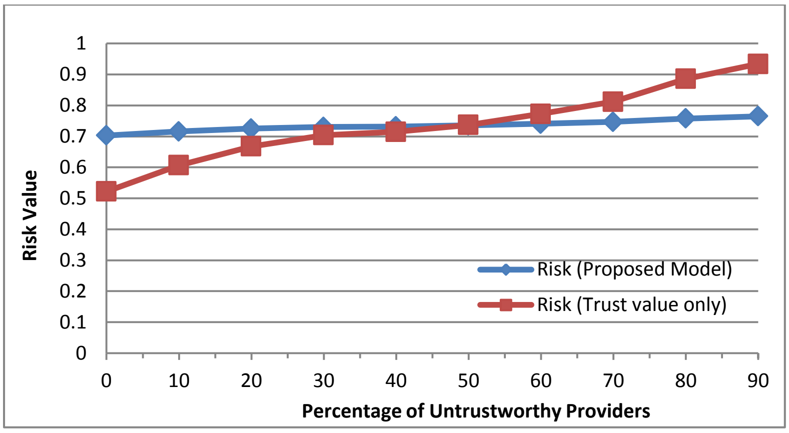


Figure 5.7: Risk result when weighted service cost =1, warranty =1 and trust value = Not relevant

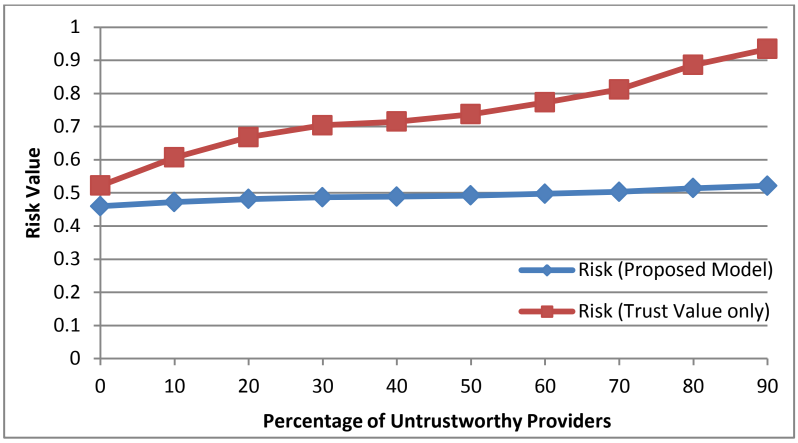


Figure 5.8: Risk result when weighted service cost=1, warranty =0.33 and trust value = Not relevant

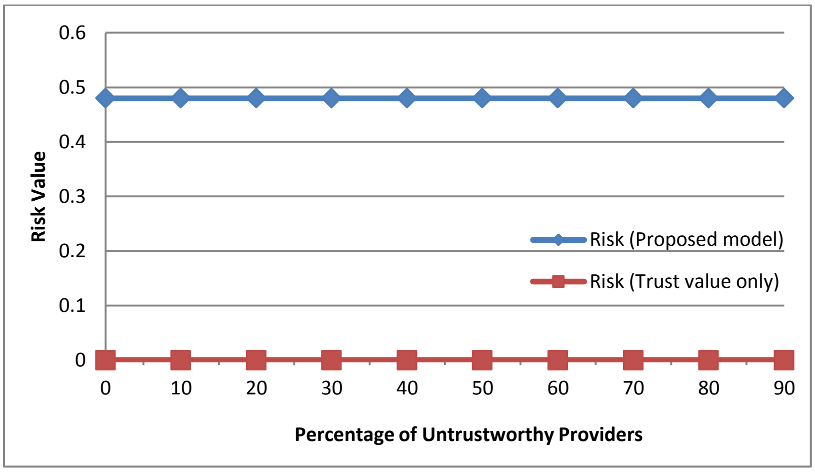


Figure 5.9: Risk result when weighted service cost=0.1, warranty =1 and trust value =0

Figure 5.6, Figure 5.7 and Figure 5.8 show results when trust value of service providers is not relevant to the potential transaction. Figure 5.9 shows when service providers are new in the marker with no trust value. The result shows that the risk indication of the proposed model is higher than the trust reputation-based model at the first half of the result. And all the figures also show that when the percentage of untrustworthy service providers increases the differences of the resulting risk value of the two models increases as well. This is because of the fact that although trust value is one of the important parameters in transaction risk value assessment, it should not be the only parameter used in transaction risk assessment in online environments. Also, the consistency of the risk values under varying percentage of untrustworthy service providers demonstrates the importance of the product properties (i.e., cost and warranty) when computing the transaction risk values. It also demonstrates the advantage of the proposed model, which shows its ability to produce a risk level even when there is no trust value of service providers such as a new service provider. For example, in reputation-based systems, trust value is accumulated from feedback ratings from buyers who have transaction experience with the service providers. These trust value is used to estimate the risk of buying from the individual service provider. The higher the trust value of a service provider indicates the lower the risk of future transaction. However, when service providers change their behavior, buyers might not have immediate information as the trust values take time to accumulate. This model will enable buyers to use the risk indicator to have immediate result rather than cumulative, and does enhance the accuracy of risk information.

5.6 Chapter Summary

In this chapter, we proposed a risk-based trust management system that helps online shoppers decide whether or not to proceed with a given transaction. Unlike the existing systems that solely depend on a single value to determine the trustworthiness of a product, we proposed a multi-attribute trust management system that takes into account both product properties and the service providers historical trust in computing the risk level of the transaction.

The advantage of our trust model is that it enables potential users identify the risk associated with a given transaction rather than based on the reputation of service providers. For example, in reputation system, trust value is accumulated from feedback ratings from buyers who have transaction experience with the service providers. These trust value is used to estimate the risk of buying from the individual service provider. The higher the trust value of a service provider indicates the lower the risk of future transaction. However, when service providers change their behavior, buyers might not have immediate information as the trust values take time to accumulate. Risk assessment cannot help people establish trust on eCommerce environment because it only informs people of the risk they may take. Our model combine both risk and trust will enable buyers to use the indicator to have immediate result rather than cumulative, and does enhance the accuracy of risk information.

We have studied the effectiveness of the system through simulation and compared it with a standard reputation based systems. The results of the experiment demonstrate that the multi-attribute based system outperforms the tradition reputation-based systems. Furthermore, multi-attribute based system is able to provide risk indication for online buyer when there is no trust value of a new service provider. In view of the above, our trust model presents an alternative approach to avoid financial loss on buying goods online.

Chapter 6

Summary and Future Directions

In this chapter, the contributions and findings of the thesis are summarized, followed by a list of research issues for future investigations and improvements.

6.1 Summary of contributions

Trust plays and will continuously play an important role in eCommerce. It is widely addressed as an important issue in eCommerce environment. The rapid growth of new technologies of Internet services introduces new requirements and challenges to eCommerce trust management. This research identifies important trust issues that can be implemented to enhance trust. It mainly focuses on discussing several important topics related to eCommerce. It has studies methodologies and trust mechanisms of eCommerce trust management. The areas of trust modelling, feedback credibility and trust evaluation methods are also addressed. In addition, solutions to further enhance the reliability of eCommerce trust management system are proposed. This thesis contributes in the following four aspects.

Firstly, an extensive literature survey on the various components required for designing an eCommerce trust management system model was conducted. It first gives an overview of the existing works and approaches to trust management. The understanding generated from the literature survey shows that reliable trust management system still remains an open and challenging problem. This study instructs our work towards solving special issues of trust management in the eCommerce environment. The analyses of these trust management issues faced by users engaged in eCommerce were presented. We found that the current trust management system lacks of a consistent model to help manage trust. It also lacks a practical approach that could help us design and develop a usable trust management system. In addition, the existing techniques of trust assessment are susceptible to trust management due to the vulnerability of eCommerce environment. It needs further improvement in order to enhance the current eCommerce trust management.

Secondly, the extensive literature review on trust management provides directions in finding the requirements of a reliable trust modelling and its methodology. A conceptual architecture to clarify the structure of trust issues in eCommerce is presented. The threats and challenges to eCommerce as well as useful information for dealing with these issues are further addressed in detail. A multilevel trust management framework is developed to improve the existing trust modelling, which includes a rating collection component, a feedback verifying component that distinguishes the feedback credibility, trust evaluation component and security mechanism for trust feedback assessment and storage. A case study is presented to validate the framework. This framework has shown that the proposed trust properties are important and improves ways on trust management in eCommerce environment.

Particularly, the conceptual multilevel architecture research provides us a clearer guideline of research steps and helps discovery mechanisms for managing trust. It helps researchers to come up with better formalization and computational solutions.

Thirdly, the contribution in the thesis is that an approach that verifies suspicious feedbacks with the aims of identifying and actioning those feedback-related vulnerabilities is designed. I addressed the problem of feedback-related trust management systems vulnerabilities as such users re-enters with a new identity and initial window where there is not enough information for trust evaluation, etc. The approach applies an appropriate filtering technique to the collected data, which assists in assigning an appropriate weight to the feedback ratings of different participants regarding a prospective service provider. It combines majority ratings and others parameters such as the amount of transaction and the number of ratings submitted by the same participant to mitigate the re-entry and value imbalance issues. This approach avoids shortcomings such as the normal ratings are separated from suspicious ratings. Also, instead of discarding suspicious ratings, a trust metric scheme is proposed to eliminate the issue of ratings sparse and discourage and reduce the impact of suspicious ratings. The results indicate that different evaluation functions are effectively supported within the proposed framework. This approach helps trust management system made smother and safer transactions.

Finally, the thesis further developed a solution that incorporates trust, transaction costs and product warranties. The focus of this multi-attribute trust management model is to augment potential online buyers' decision making process by exposing the potential risk levels of a given transaction to them. Risk assessment cannot help people establish trust in eCommerce environment because it only informs people of the risk they may have to undertake. The model by combining both risk and trust enables buyers to use the indicator to receive immediate result rather than cumulative result, and also enhances the accuracy of risk information. This new multi-attribute risk technique informs potential buyers of the risk level associated with a given product. It enables potential buyers to determine the risk level of a product before committing to proceed with the transaction. I have studied the effectiveness of the system through simulation and compared it with a standard reputation based systems. The results of the experiment demonstrate that the multi-attribute based system outperforms the tradition reputation-based systems. In addition, the proposed trust mechanisms discussed in both chapter 4 and chapter 5 can be applied together to provide a better trust results and thus enhance the reliability of eCommerce trust management system.

6.2 Future Directions

Although this thesis has answered some of the trust management issues relevant to eCommerce, it opens up a range of research problems for future work. I proposed several pieces of work worth further study and research.

1. To solve the first research issue, I have developed a framework that presents a conceptual architecture with proposed desire properties that expect to improve trust assessments. Detail of this framework has been discussed in chapter 3. It suggested that security mechanisms are necessary to prevent from malicious attacks from the eCommerce participants. It allows security mechanisms in the system to improve the accuracy of trust values. Secure trust data storage and secure communication between the services and the trust management service instances are to prevent users from impersonating a legitimate service to report false feedback and initiate a flood of trust evaluation requests. I believe an integrated solution is very promising that combines traditional security solution with the developed trust evaluation management together. The proposed framework has assumed that it is able to compute trust by combining different types of information sources. The assumption is that the infrastructure hosting the services issues digital certificates to each service and trust management service instance enables public key cryptography for confidentiality and authentication. However, in a practical situation, the interconnection of the proposed properties may not be so easily implemented. It is worth to further investigate into the performance over a practical implementation of this framework.

2. The chapter four of this thesis introduces a feedback verifying scheme for enhancing eCommerce trust management reliability. This scheme identifies malicious ratings and takes action to the ratings to improve the accuracy of trust evaluation. The result of this scheme is effective and more stable compared to the majority vote models in evaluation. It is worth trying the scheme with other trust models on other potential malicious strategies, and their effects on the methods tested, such as model of game theories approach, fuzzy logic approach etc to have an insight into the change of performance levels.
3. I have developed a risk based trust evaluation scheme which is introduced into eCommerce business as a key indicator to control the uncertainty. The detail of the scheme is presented in chapter five of this thesis. It will be valuable to the trust management if the scheme can be designed in a way to increase the scalability trust in eCommerce. Further research is required to validate the proposed model with considering this factor.
4. To satisfy the increasing demands of the growing number of feedbacks, a trust system should be established quickly and efficiently. Currently, the process is time consuming and the maintenance of databases is costly. Further investigation in improving the performance and reducing the cost of our method and compare it with existing methods can be valuable to trust management.
5. So far, all the work presented in chapter 3, 4 and 5 in this thesis has focused only on eCommerce trust management systems. However, due to the increasing number of mobile users, it would be beneficial to look at its

applicability through applying to a trust management concept in mobile applications. Taking rating based trust mechanism from standard eCommerce applications to mobile communities poses additional requirements especially on decentralised management and security aspect. It should include enabling the trust assessment at runtime and monitor of a number of attributes of the assessed users as trust value changes over time. How to manage trust in mobile applications is an interesting area and worthy of further study.

Apart from these above work mentioned, it is also a beneficial direction to include a user interface in mobile applications supporting human intervention in collecting information for trust evaluation.

References

[1] J. Abawajy and A. Goscinski. A Reputation-Based Grid Information Service. *Lecture Notes in Computer Science.* Vol 3994, pp. 1015-1022, 2006.

[2] A. Abdul-Rahman and S. Hailes. Supporting Trust in Virtual Communities. *In proceedings of the 33rd Hawaii International Conference on System Science* (Maui, HW, USA), 2000

[3] Amazon.com (2011) available at http:// www.amazom.com (access on 10th June, 2011)

[4] S. Amland. Risk based Testing and Metrics. *International Conference on Testing Computer Software*, Washington, D.C., USA, 1999.

[5] S. Balachander. Warranty signalling and reputation. *Management Science,* 47(9), pp. 1282-1289, 2001.

[6] P. Benassi. TRUSTe: An online privacy seal program. *Communications of the ACM, 42*(2), 56. 1999.

[7] M. Blaze, J. Feigenbaum and J. Lacy. Decentralized Trust Management. *Conference on Security and Privacy Proceedings Symposium,* pp164 – 173, 1996.

[8] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The KeyNote Trust management System Version 2. RFC 2704, *The Internet Society*. http://www.faqs.org/ftp/rfc/pdf/rfc2704.txt.pdf ,1999

[9] J. Breese, D. Heckerman, and C. Kadie. Empirical analysis of predictive algorithms for collaborative filtering. *In Proceedings of the 14th Conference on Uncertainty in Artificial Intelligence (UAI-98),* pp 43-52., 1998.

[10] J. Brownlie and A. Howson. Leaps of Faith and MMR. *An empirical Study of Trust, Sociology* 39:221-239, 2005

[11] S. Buchegger and J.Y. Le Boudec. The effect of Rumor Spreading in Reputation system for mobile Ad hoc Networks. *In proceedings of the workshop on modelling and optimization in mobile. Ad Hoc and wireless Networks*. March, 2003

[12] S. Buchegger and J.Y. Le Boudec. A Robust Reputation System for Mobile Ad-hoc Networks.*Technical report IC/2003/50, EPFL- IC-LCA,* 2003

[13] J. Bus. Building trust and security in information society. *A strategic challenge for European RandD. ERCIM News Online Edition,* ERCIM News, 63, October 2005.

[14] R. Buyya, J. Giddy, and D. Abramson. An Evaluation of Economy-based Resource Trading and scheduling. *Computational Power Grids for Parameter Sweep Applications*, July, 2000.

[15] C. Castelfranchi, R. Falcone and G. Pezzulo. Trust in Information Sources as a Source for Trust. *A Fuzzy Approach. AAMAS, pp. 89-96*, 2003

[16] S. Charney. Establishing end to end trust, Microsoft Corp Available at http://download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf., 2008. Access on March, 2012.

[17] C. H. Cho, H. J. Cheon, & J. Kang. Online Shopping Hesitation. *Cybersychology & Behavior*, *9*(3), 261-274, 2006.

[18] S-K.Chong and J. Abawajy. Risk-Based Trust Management for E-Commerce. In Z. Yan (Ed.), *Trust Modeling and Management in Digital Environments: From Social Concept to System Development*, pp: 332-351, 2010.

[19] A. Chonka, S.K. Chong,W.Zhou, and Y.Xiang. Multi-core Security Defense System (MSDS). *IEEE The Australasia Telecommunications Networks and Applications Conference, IEEE,* 2008

[20] S.Choudhury, S. D. Roy, and S. A. Singh, Trust Management in Ad Hoc Network for Secure DSR Routing, Novel Algorithms and Techniques. *InTelecommunications, Automation and Industrial Electronics. Springer Netherlands* pp. 496-500, 2008.

[21] Consumer Report. Why don’t you need an extended warranty. Retrieved August 20, 2008, from http://www.consumerreports.org/cro/money/news/november-2006/why-you-dont-need-an-extended-warranty-11-06/overview/extended-warranty-11-06.htm

[22] R. P. Crease. The paradox of trust in science', in *Physics World*. Pp. 18, 2004

[23] C. Dellarocas. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In *Proceedings of the 2nd ACM conference on Electronic commerce* (pp. 150 - 157), 2000.

[24] C. Dellarocas. Efficiency through feedback-contingent fees and rewards in auction mar- ketplaces with adverse selection and moral hazard. San Diego, CA, USA. *Proceedings of the 4th ACM Conference on Electronic Commerce*., 2003.

[25] W. DeLone and E. McLean. Measuring eCommerce Success: Applying the DeLone and McLean Information Systems Success Model, *International Journal of Electronic Commerce,* Vol. 9, Iss. 1, pp 31 – 47, 2004.

[26] M. Deutsch. Cooperation and Trust: Some Theoretical Notes. *Nebraska Symposium on Motivation, Nebraska University Press, Nebraska University Press*. pp275–319,1962.

[27] J. Donath, Identity and Deception in the Virtual Community, *Communities in Cyberspace,* Kollock, P. and Smith M. (eds). London: Routledge, 1998.

[28] J. O'Donovan, B. Smyth, V. Evrim and D. McLeod Extracting and Visualizing Trust Relationships from Online Auction Feedback Comments. In *Proc. IJCAI '07*, 2826–2831, 2007.

[30] C. Duma and N. Shahmehri. Dynamic Trust Metrics for Peer-to-Peer Systems. *16th International Workshop on Database and Expert Systems Applications,* pp. 776-781, 2005.

[31] eBay 2011, eBay,com available at http://www.ebay.com/

[32] E-business versus eCommerce. Available at http://www.austrade.gov.au/e-business-versus-eCommerce/default.aspx. access on 8-8-2011

[33] eMarketer. (2007). *Canada B2C ECommerce*. Mindbranch. Retreived December 10, 2008, from http://www.mindbranch.com/Canada-B2C-Commerce-R203-462/

[34] Forrester Research. (2007). *Total Online Sales Expected To Hit $259 Billion In 2007 Washington*. Retreived January 5, 2009, from http://www.forrester.com/ER/Press/Release/0,1769,1145,00.html

[35] D. Gambetta. Can We Trust Trust? *Oxford, UK: Basil Blackwell,*1990.

[36] E. A. Greenleaf, & D. R. Lehmann. Reasons for substantial delay in consumer decision making. *Journal of Consumer Research, 22*, 186-199, 1995.

[37] D.Goldberg, D. Nichols, B.M. Oki, D. Terry. Using collaborative filtering to weave an information tapestry. *ACM Commun. 35(12),* pp 61–70, 1992

[38] T.Grandison and M. Sloman. A Survey of Trust in Internet Applications. *IEEE Communications Survey and Tutorials,* 4(4), pp. 2-16, 2000.

[39] D.G. Gregg and J.E. Scott. A Typology of Complaints about Ebay Sellers. *CACM*. 51 (4), 2008.

[40] Gulcher JR, Kristjansson K, Gudbjartsson H, and Stefanson K. Protection of privacy by third-party encryption in genetic research. *Eur J Hum Genetics*, 8: pp739-742, 2000.

[41] Hall, M. A., E. Dugan, B. Zheung, and A. K. Mishra. Trust in Physicians and Medical Institutions: What IS IT, Can It Be Measured, and Does It Matter?', *The Milbank Quarterly* 79:pp 613-639, 2001.

[42] R. Henderson, D. Rickwood, and P. Roberts. The beta test of an electronic supermarket. *Interacting with Computers, 10,* 385-399, 1998.

[43] L. H. Huang, Z. J. Zhong and D. N. P. Murthy. Optimal reliability, warranty and price for new products. *IIE Transactions, 39*(8), pp819-827, 2007.

[44] S.D. Hunt and D.F. Davis. Grounding supply chain management in resource-advantage theory. *Journal of Supply Chain Management* , 44(1): pp 10-21, 2008.

[45] T. D. Huynh, Trust and Reputation in Open Multi-Agent Systems, PhD thesis, *University of Southampton*, 2006.

[46] Ic3. (2009). *Reported Dollar Loss From Internet Crime Reaches All Time High*. Retrieved July 10, 2011, from http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

[47] P. Ifinedo. Enterprise Systems Success Measurement Model: A Preliminary Study. *Journal of Information Technology Management*, Vol. 17, Iss. 1, pp 14 – 33, 2006.

[48] S.L. Jarvenpaa and P.A. Todd. Consumer reactions to electronic shopping on the World Wide Web. *International Journal of Electronic Commerce, 1*(2), pp 59-88, 1996.

[49] C. M. Jonker and J. Treur. Formal Analysis of Models for the Dynamics of Trust Based on Experiences. In *Proceedings of the 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World: Multi-Agent System Engineering*, pp. 221-231,1999.

[50] A. Jøsang and R. Ismail. The beta reputation system. In: *Proceedings of the 15th bled electronic commerce conference.* pp 1–14, 2002.

[51] A. Jøsang, E. Gray and M. Kinateder. Simplification and Analysis of Transitive Trust Networks. *Web Intelligence and Agent Systems Journal*, 2006.

[52] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision, *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, 2007.

[53] A.Jøsang and J. Golbeck. Challenges for Robust of Trust and Reputation Systems. *Proceedings of the 5th International Workshop on Security and Trust Management (STM 2009).* Saint Malo, France, September 2009.

[54] A. Jøsang, and S. LoPresti. Analysing the Relationship between Risk and Trust. In *Trust Management* Berlin, Germany: Springer. Pp.135-145, 2004.

[55] A. Jøsang and W. Quattrociocchi, Advanced features in Bayesian reputation systems, in *Trust, Privacy and Security in Digital Business*, vol. 5695, Heidelberg: Springer, pp. 105-114, 2009.

[56] R. Jurca and B. Faltings. An Incentive Compatible Reputation Mechanism. In *Proceedings of the 6th International Workshop on Deception Fraud and Trust in Agent Societies (at AAMAS'03)*pp. 1026-1027, 2003.

[57] R. Kerr and R. Cohen. Modeling trust using transactional, numerical units. In *PST '06: Proceedings of the Conference on Privacy, Security and Trust,* Markham, Canada, 2006.

[58] R. Kerr and R. Cohen. Smart cheaters do prosper: defeating trust and reputation systems. In *Proceeding AAMAS '09 of the 8th International Conference on Autonomous Agents and Multiagent Systems*, Vol (2), 2009.

[59] P. Kollock, The Production of Trust in Online Markets. *Advances in Group Processes* (Vol. 16), edited by E. J. Lawler, M. Macy, S. Thyne, and H. A. Walker. Greenwich, CT: JAI Press. 1999.

[60] C.L.Lee and S.Q. Lai. Performance measurement systems for knowledge management in high technology industries: a balanced scorecard framework. *International Journal of Technology Management,* 39 (1/2) pp. 158–176, 2007.

[61] P.M. Lee. Behavioral Model of Online Purchasers in E-Commerce nvironment. *Electronic Commerce Research, 2*(1-2), pp75-85, 2002.

[62] M.K.O. Lee and E. Turban. A trust model for consumer Internet shopping. *International Journal of Electronic Commerce* **6(**1), pp 75–91, 2001.

[63] J. Love. Comments to the Australian AG's on the proposed Hague Convention *on Jurisdiction and Foreign Judgments* (Issues paper 3). Australian Consumers' Association. (2001). Retrieved March 3, 2009, from http://lists.essential.org/pipermail/hague-jur-commercial-law/2001-February/000009.html

[64] N. Luhmann, (Ed.). *Trust: making and breaking cooperative relations*. Oxford, UK: Blackwell, 1990.

[65] B. Malin and L. Sweeney. How (not) to protect genomic data privacy in a distributed network: using trail re- identification to evaluate and design anonymity protection systems. *Journal of Biomedical Informatics* vol 37, pp 179–192, 2004

[66] D. W. Manchala. E-Commerce trust metrics and models. *Journal Internet Computing, 4*(2), 36-44, 2000.

[67] D. H. McKnight, L. L. Cummings and N. L. Chervany. Initial Trust Formation in New Organizational Relationships. *Academy of Management Review, 23*(3), pp 472-490, 1988.

[68] G.J. de Moor, B. Claerhout, F. de Meyer. Privacy enhancing technologies: the key to secure communication and management of clinical and genomic data. *Meth Info Med* 2003; 42: 148-153.

[69] D. N. P. Murthy and W. R. Blischke (Eds.). *Warranty Management and Product Manufacture*. London: Springer Verlag, 2005.

[70] L. Nancy, Carter and J. Mark Weber Not Pollyannas : Higher Generalized Trust Predicts Lie Detection Ability. *Social Psychological and Personality Science* 2010 1: 274

[71] Pew Internet. *Online shopping survey*. Retrieve from www.pewinternet.org /Reports/2008/Online-Shopping.aspx, access on 2nd Nov. 2010.

[72] S. Pittayachawan, M. Singh and B. Corbitt. A multitheoretical approach for solving trust problems in B2C e-commerce. *International Journal of Networking and Virtual Organisations*, 5 (3), pp. 369-395, 2008.

[73] L. Price, and N. Dawar. The Joint Effects of Brands and Warranties in Signaling New Product Quality. *Journal of Economics Psychology,* vol 23, 165-190, 2002.

[74] I. Raza and S.A. Hussai, 2008. Identification of malicious nodes in an AODV pure ad hoc network through guard nodes. *Computer Communications*, vol 31, Issue 9, pp. 1796-1802, 2008,.

[75] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation Systems. *Communications of the ACM*, December, Vol 12: pp. 45-48, 2000.

[76] P. Resnick and R. Zeckhauser, (Eds.). *Trust among strangers in internet transactions: empirical analysis of eBay's reputation system*. Vol. 11, 2002.

[77] P. Resnick,and., R. Zeckhauser (Eds). Trust among strangers in internet transactions: empirical analysis of eBay's reputation system, Vol. 11, 2006.

[78] J. Sabater, and C. Sierra, Social ReGret, A reputation model based on social relations. *SIGecom Exchanges*, vol. 3, no. 1, pp. 44-56, 2002.

[79] J.Sabater and C. Sierra. Reputation and social network analysis in multi-agent systems. *Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent System (AAMAS 2002),* Bologna, Italy, 15-19 pp. 475-482, July 2002,

[80] J. Sabater. Evaluating the ReGret System. *Applied Artificial Intelligence*, Volume 18, Issue (9-10), UK, pp.797-813, 2004

[81] I. Sahin and H. Polatogu. *Quality, Warranty and Preventive Maintenance*, Kluwer Academic Publishers, Norwell, MA, 1998.

[82] S. Sajjan, R. Sankardas and D. Dasgupta. Game Theory for Cyber Security. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010.

[83] J. Saranow. DaimlerChrysler Goes in Reverse on Warranties, *The Wall Street Journal*, May 26, 2005.

[84] D. F. Schoorman, R. C. Mayer and J. H. Davis. An Intergrative Model of Organizational Trust: Past, Present, and Future, *Academy of Management Review* 32:pp 344-354., 2007

[85] G. Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, Princeton and London, 1976.

[86] C. Shapiro. Consunmeer Information, Product Quality, and Seller Reputation. *The Bell Journal of Econmics*, 13(1):pp 20-35, 1982.

[87] S. Shiva, S. Roy, H. Bedi, D. Dasgupta, and Q. Wu. An Imperfect Information Stochastic Game Model for Cyber Security. *The 5th Intnl Conference on i-Warfare and Security*. 2010.

[88] B. Stahl. Trust as Fetish: A critical Theory Perspective on Research on Trust in Ecommerce. *Journal of Information, Communication Society, 10th Anniversary International Symposium,* York, 2006.

[89] R. L. Standiferm and A.W. Jr. James. Managing conflict in B2B eCommerce. *Business Horizons*, *46*(2), pp65-70., 2003.

[90] M. Tavakolifard, S. J. Knapskog, and P. Herrmann. Trust transferability among similar contexts. In *ACM Q2SWinet*, pp 91–97., 2008.

[91] J. Trevathan and W. Read. Undesirable and Fraudulent Behavior in Online Auction. *SECRYPT'06*, pp 450-458, 2006.

[92] J. Trevathan and W. Read. RAS: *a system for supporting research in online auctions, ACM Crossroads*, ed. 12.4, 23-30, 2006

[93] J. Trevathan, and W. Read. A Simple Shill Bidding Agent. *Proceedings of the Fourth International Conference on Information Technology (ITNG'07*), pp.766-771, 2007.

[94] U.S. Census Bureau. *Annual Retail Trade Survey – 2007*. Retreived December 10, 2008, from http://www.census.gov/svsd/www/artstbl.html

[95] T. Vu, P. Smith and T. Bennett. *BizRate.com, NPD Joint Survey Reveals 75 percent of Online Customers are Abandoning Shopping Cart*. (1999). Retrieved March 5, 2009, from http://www.highbeam.com/doc/1G1-56901280.html

[96] Y, Wang, Q. Zhang and Y. Jiang. A Trust Management Model based on Multi-agent System1. *ISECS International Colloquium on Computing, Communication, Control, and Management*. 2008.

[97] T. Wang, T. Tang and J. Tang. An Instrument for Measuring Customer Satisfaction toward Web Sites that Market Digital Products and Services, *Journal of Electronic Commerce Research*, Vol. 2, Iss. 3, pp 20-48, 2001.

[98] Web Transitions, Inc. (2004). *Advantages of an eCommerce website*. Virginia: Boons Mill. Retrieved March 5, 2009, from http://www.letmeshop.com/eCommerce-design-info/advantages-of-eCommerce.asp

[99] A. Whitby, A. Josang, and J. Indulska, Filtering out malicious ratings in Bayesian reputation system. In *proceeding 7th Int. workshop on Trust in Agent Societies*, 2004.

[100] Q. Wu, S. Shiva, S. Roy, C Ellis, and V. Datla. *On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks*, SpringSim, 2010.

[101] L. Xiong and L. Liu. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. Knowl. Data Eng. (TKDE)* 16(7), pp 843–857, 2004.

[102]Y. Yang, Y. Sun, J.Ren, and Q.Yang. Building trust in online rating systems through signal modeling. In *Proceedings of IEEE ICDCS workshop on Trust and Reputation Management*, 2007

[103]B. Yu, and M. Singh. Detecting deception in reputation management. Proceedings of *the second international joint conference on Autonomous agents and multiagent systems*, pp73-80, 2003.

[104] B. Yu, M. Venkatraman, and M. P. Singh. An Adaptive Social Network for Information Access: Theoretical and Experimental Results, *Journal of Applied ArtificialIntelligence*, 2003.

[105] B. Yu and M. P. Singh. Searching Social Networks, *Second International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2003.

[106] B. Yu, P. M. Singh and K. Sycara. Developing Trust in Large-Scale P2P Systems. *Proceedings of First IEEE Symposium on Multi-Agent Security and Survivability*. pp. 1-10, 2004.

[107] G. Zacharia, A. Moukas and P. Maes. System Sciences,. HICSS-32. *Proceedings of the 32nd Annual Hawaii International Conference* Volume 8, pp(s):7, 1999

[108] H. Zhang, Y. Wang and X. Zhang. Transaction Similarity-Based Contextual Trust Evaluation in E-Commerce and E-Service Environments. *Journal of Computer Science and Technology* 24(5): 883- 892 Sept. 2009

[109] J. Zhang, and R. Cohen. Trusting advice from other buyers in e-marketplaces: the problem of malicious ratings. In *Proceedings of the 8th international conference on Electronic commerce*, 2006.

[110] J. Zhang and R. Cohen. Design of a Mechanism for Promoting Honesty in E-Marketplaces. In *Proceedings of the Twenty-Second Conference on Artificial Intelligence (AAAI-07);* pp. 1495-1500, 2007.

[111] M. Zuo, J-H Li and G-S Liu. An Adaptive Collaborative Filtering Algorithm for Online Reputation Systems in *Third International IEEE Conference on Signal Image Technologies and Internet Based System*, 2007.

[112] Zicasso. Retrieved 10 Mach 2012, from: http://www.zicasso.com/