Chapter 2

Related Works

Trust and reputation are complex and interdisciplinary in nature. A concise and universally accepted definition of trust has remained elusive, and the concept of trust is usually based on analysis from the viewpoint of a single discipline. We explore how these concepts are defined in multiple disciplines so that its complex and subjective nature can be understood.

2.1 Overview of Trust and Reputation

2.1.1 Defining Trust

2.1.1.1 Trust in Psychology

In psychology, the most popular and widely accepted definition of trust given by Deutsch [20] states that "*trusting behaviour takes place when an individual confronts an ambiguous path leading to a perceived either beneficial or harmful result contingent on the action of another person*." Jøsang et al. [21] in their definition of trust state that "*Trust is the subjective probability by which an individual expects that another performs a given action on which its welfare depends.*" These definitions emphasise that trust occurs when an individual believes the trusted other will act in an expected way, and the future action is committed by the individual based on that belief.

2.1.1.2 Trust in Sociology

Trust in sociology has many meanings. Trust is a means of overcoming the complexity of a society. Furthermore, trust is an emergent characteristic of relationships between social entities, both individuals and groups. Thus, the

meaning of trust in sociology is defined at individual level and at societal level. The meaning of individual level trust is similar as the ones from psychology [22, 23]. For example, Sztompka [24] proposed a general definition of trust as "Trust is a bet about the future contingent actions of others," which is similar to the definition given by Deutsch [20] in Psychology. Belief and commitment are two main components of this definition. Trust occurs when that belief that the trusted person will act in certain way is used as the foundation for making a commitment to a particular action. At this level, the specific trust between two interacting parties is termed as "relational trust", which is built up through their repeated direct interactions and declines when betrayed [22].

At the societal level, trust is considered as a property of social groups. Luhmann [25] considers trust as "a means for reducing the complexity of society". A more detailed definition from Seligman [26] states that "trust enters into social interaction in the interstices of systems, when for one reason or another systematically defined role expectations are no longer viable. If people play their roles according to role expectations, we can safely conduct our own transaction accordingly". Any gap between roles and role expectations brings forth trust (distrust) problems. At the societal level, the term "generalized trust" [27] is used to mean the general belief of the trustor towards a group of members that it acts as expected. For example, professors are always considered professional in their research fields.

In human society, the generalized trust initializes the trust relationship between two unfamiliar parties, and offers an opportunity for establishment of relational trust through forthcoming interactions between them. Moreover, Marsh [28] declares that inevitable loss of understanding trust as both personal and social concepts will be resulted from ignoring either rational or generalized trust.

2.1.1.3 Trust in Economics

From economics perspective, the European Commission Joint Research Center [29] defines trust as "trust is the property of a business relationship, such that

reliance can be placed on the business partners and the business transactions developed with them." This definition is from the perspective of business management which implies the importance of trust in commercial activities. Another important conceptualisation of trust is that it is a measure of reliability in transactions [30]. More precisely, Akerlof [31] points out that trust affects economic costs. Ba et al. [32] demonstrate that trust can reduce transaction risks, mitigate information asymmetry and generate price premiums for reputable vendors. This phenomenon is quite evident in online trading environments, such as e-commerce and e-service, where consumers cannot directly interact with products and workers, and the credibility of online information may be doubtful [33]. The quality of products cannot be judged in advance because the online information is mainly posted by the vendors themselves. Thus, trust is considered by some economists as a mechanism to restrict opportunistic behaviour and establish a reciprocal relationship between consumers and vendors.

2.1.1.4 Trust in Computer Science

Trust is a widely used term with various definitions among researchers across different fields of computer science. As a reference point for understanding the concept of trust in computer science, three definitions can be taken up. The first definition used by Mui et al. [35] states that "Trust is a subjective expectation an agent has about another's future behaviour based on the history of their encounters". This definition refers to past encounters, and is widely accepted as reputation-based trust. Reputation-based trust uses an entity's past interactions or performance to compute trust for assessing its future behaviour, and may utilize referral based trust i.e. information from others in the absence of or in addition to first-hand knowledge [36]. For example, when a consumer purchases a product from an unknown eBay vendor, the initial trust is established only based on the experiences (ratings) of others. The second definition is from Grandison and Sloman [58]. They define that "Trust is the firm belief in the competence of an entity to act dependably, securely, and reliably with a

specified context". This definition introduces context of trust. The third definition from Olmedilla et al. [54] states that " Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context of the service X" Bonatti et al. [34] categorize trust using reputation and policy. On the contrary, policy-based trust is established, when sufficient necessary conditions are met, to control access rights [36]. It is founded on logical rules and verifiable properties encoded in digital credentials [34]. The aim of policy-based trust is to determine whether an unknown participant can be trusted or not based on a certain number of credentials and a set of relevant policies. Moreover, in computer science, a number of various trust prediction models are designed to help establish trust relationships by simulating the process of trust establishment among people in human society. For example, Marsh [28] proposes a set of variables and a method to incorporate them all into a continuous value in the range of [-1; 1] to represent trust.

From the aforementioned different trust definitions, we can see that depending on the environment in which trust is being specified, it is composed of attributes like reliability, dependability, honesty, truthfulness, security, competence, and timeliness.

2.1.2 Defining Reputation

Reputation as a social concept is more easily defined than trust. While trust always includes a subjective element based on the disposition of the trust origin, reputation can be measured from an accumulation of independent experience-based opinions, i.e. recommendations, resulting in an evaluation of the overall character of an entity.

In [109] reputation is defined as "*what is generally said or believed about a person's or thing's character or standing*", and they purport that reputation can be quantitatively measured from information in an underlying social network. This information is visible to all members of the network. Therefore, in a

situation where personally-observed evidence is lacking for a given entity, in some instances it is possible to seek out recommendations about that entity from one or many trusted third parties. Recommendations from third parties, when accumulated, constitute an entity's reputation that can be used in the absence of personal experience to make a decision about an entity's character.

Abdul-Rahman and Hailes[60] extend this definition to include the notion of using reputation to search out entities that are characterised by evidence about a particular behaviour, stating that a "*reputation is an expectation about an agent's behaviour based on information about or observations of its past behaviour*".

Elezabeth Chang, et.al. [108] defined the reputation in SOA as "the third party recommendation agents' opinion in response to the reputation query for the trustworthiness of the trusted entity (such as trusted agent or QoP or QoS)"

From this definition it is clear that reputation value is calculated based on the recommendations presented by the third party agents via a reputation query.

In general, a reputation is a collection of recommendations, i.e., personal observations recommended by one or more third parties, about an entity's past behaviour which are accumulated in such a way as to characterise an entity's nature with regard to ability or reliability in potential future interactions in a given context. If the accumulated recommendations are evidences of behaviour for a given trust purpose, then the resultant reputation characterising an entity's trustworthiness can be used as input to a trust-based decision-making system. Such a system could then perform trust-based reputation management such that a security decision as to whether or not to interact with a given entity might be provided to users.

2.1.3 Properties of Trust

After reviewing the definitions of trust in different disciplines, a set of general properties that are believed to be significant to the study of trust prediction can

be crystallised. These properties of trust provide the theoretical foundation for the design of various trust prediction approaches.

2.1.3.1 Trust is subjective

In social psychology [37, 38], trust is an individual's subjective opinion towards another individual based on his/her own psychological experience, evaluation and the domains of both. Even the trust towards the same individual can vary significantly. For instance, Alice trusts Bob based on her good experience during all the historical interactions with Bob. But, Cathy distrusts Bob because of a betrayal. Golbeck [39] provides another example that the population split significantly when asked about whether or not to trust the current President's effective leadership.

In computer science too, subjectivity is one of the major properties of trust [40]. Jøsang [41, 42] leverages subjective logic to explain trust and further explains that an opinion can be uniquely described from belief, disbelief and uncertainty. Moreover, the subjective property is also applied to evaluate the trustworthiness of a vendor in online trading environments, such as e-commerce [43]. For instance, eBay provides a rating system to assist vendors and buyers. A buyer can provide a rating (+1, 0, or -1) after each transaction regarding to the transaction quality. In particular, a number of mathematical models have been proposed to model the changes of subjective trustworthiness, such as the Beta model [44] and the Markov chain model [45]. In addition, some researchers treat the subjective property as personalization, e.g., Richardson et al. [46] consider that the user ratings in a trust management system attribute to personalization.

2.1.3.2 Asymmetric

Asymmetric property of trust, also known as "one-way trust" in [37], means that trust between two parties does not necessarily exist in both directions or to the same extent. Asymmetry is mainly caused by the different roles in interactions. For example, a buyer trusts a seller because of the good experience during all

its buying interactions with the seller. But, conversely, the buyer may not trust the seller any more, if the seller starts to sell products. Again even between two trusted individuals, the amounts of trust in each other's minds can differ significantly, due to different personal experiences, psychology and backgrounds. For example, there is a two directional trust relationship between a research scholar and her supervisor but their degrees may be different. The student trusts the supervisor for her ability in the research field. However, the supervisor trusts the student in the expectation of potential good working performance. This can be seen in a variety of hierarchies [51]. In summary, trust is not reciprocal or equivalent between two entities, which must be taken into account in trust prediction (or evaluation).

2.1.3.3 Propagative

Propagation, also known as inference, is one of essential properties of trust that helps in establishing a trust relationship between unfamiliar entities. This property enables the flow of trust information in a trust path from the source to the target. For instance, if A trusts B and B trusts C, A might trust C to some extent [47, 48]. In this case, A may not even know C at all. The establishment of the trust to C in A's mind depends on both A's trust to B and B's trust to C [51, 52]. This meets the fact that while trying to establish a trust relationship with an unknown person, it is common for people to ask trusted friends for opinions about the trustworthiness of this new person [39]. Furthermore, based on the property of trust propagation, a number of trust inference models to evaluate trust from a source entity to a target entity along a trust path between them that consists of links and trust values have been founded [49]. In the propagation process, trust decays with the increase of propagation hops along a social trust path [50]. In addition, as the multiple entities and contexts are involved in a trust path, trust propagation becomes complicated [48, 52]. In computer science, it has attracted more and more researchers to study trust propagation in large-scale complex social networks [52], web application areas including e-commerce [53, 54, 55], P2P systems [56], and social networks [44].

2.1.3.4 Context Dependent

The concept of trust extensively suggests that "research on trust requires the attention to context." Oxford Dictionary defines context as "the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood". Many researchers have used this concept of context in their studies of trust. It is stated in [57] that a person's trust in another person changes regarding different contexts, because expertise of a recommender may vary in different domains. In computer science, a more specific and widely accepted definition is proposed by Dey et al. [69]: *"Context is any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and the application themselves."* In addition, Grandison and Sloman [58] used the concept of context to define trust as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". More specifically, McKnight et al. [59] in their proposed meaning of "interpersonal and personal trust" it is stated that one person trusts another person in a specific context. For example, Alice may trust Bob as a mechanic in the specific context of servicing her car but probably not in the context of babysitting her children [60]; and "Whilst I may trust my brother to drive me to the airport, I most certainly would not trust him to fly the plane!" [61]. Furthermore, Marsh [61] proposed the concept of "situational trust" to suggest that context affects trustworthiness. In addition, Mui [62] stresses that trust depends on the context in the viewpoint of reputation, and states "Bill Clinton's reputation as a politician is likely to be very different from his reputation as a cook," which means we could only trust Bill Clinton as a politician instead of a cook from past experiences. In Online Social Networks, Liu et al. [63] stated that social context depends on many attributes such as social relationship, social position, preference and residential location etc. And, trust can be transferred between relevant contexts [64]. For example, if Alice

trusts Bob in teaching Visual C (VC), Alice can also trust Bob in teaching Java to some extent, as the contexts of teaching VC and teaching Java are similar. A growing number of studies have been focusing on context in trust prediction in recent years [65, 66, 67, 68, 45].

2.1.3.5 Dynamic

Dynamic property of trust means that the trust between two entities may change over time. The trust establishment process itself has already indicated this property of trust. Rousseau et al. [22] state that trust can occur, intensify, or decay based on repeated direct interactions with new experiences, which reflects temporal characteristics of trust. Dealing with the changes of trust over time, there are three main types.

- Trust decay Method

Trust of one person on another is based on the person's experience of interactions with the later. As this experience fades over time, the trust may decay over time. In trust evaluation, newer interactions are usually more important than older ones since old experiences may become obsolete or irrelevant with time passing by. Based on this characteristic, researchers in computer science used mechanisms to gradually reduce the influence of old interactions, or increase the weight of recent interactions, when predicting trust [70, 74, 80, 79]. In particular, Spitz et al. [72] point out a common phenomenon in e-commerce websites that sellers can have a large lapse of time since their last transactions, in which the decay of trust over time is more essential.

- Trust Window method

Trust time window is another way to deal with the dynamic characteristic of trust. For example, in the e-commerce website eBay, the time window can be set to last one month, last six months or last twelve months. Similarly, PeerTrust [76, 78] allows users to set the time window; and Shi et al. [71] propose a mechanism for dynamic peer-to-peer trust based on time-window feedback. Furthermore, in some works, the hybrid of trust decay and time window is

adopted [75, 74, 79]. Trust can fluctuate strategically and consciously change their behaviours in order to maximize personal profit [77].

- Probabilistic Trust Method

To deal with this type of difficult situations, probabilistic models are the most promising tools to deal with uncertainty. For instance, a Hidden Markov Model is leveraged by ElSalamouny et al. [81] to predict the trust of outcomes of future transactions. Liu et al. [45] propose a model based on Markov chains and context information to predict trust.

2.2 Trust and Reputation Models

2.2.1 General Models

In current research a large number of trust and reputation models have been developed for varied application areas such as electronic commerce, P2P , web search, Web service and service-oriented computing, movie recommendations etc. A good number of surveys on these models are available in the literature [9,19,21,23,36,58,84,85]. Each survey used a different parameters for analysis and categorization of trust and reputation systems. Here we make a survey and analysis of the trust and reputation systems based on their *application areas* and *computational techniques.*

We exclude the survey and analysis of Web service trust and reputation models from this section. These models are discussed separately in the next section.

2.2.1.1 Application-Based Taxonomy

E-commerce

In the virtual world of e-commerce, the issue of trust and reputation have received much attention from researchers. The most popularly known reputation

system in e-commerce are eBay and Amazon. With the increase in research studying reputation-based trust evaluation approaches, other models like [126, 35, 56, 65], the Sporas and Histos systems are introduced. The Sporas system takes into account dynamic property of trust, and the ratings of later transactions are given higher weights. The Histos system used both direct experience and the reputation. In P2P e-commerce environments, Xiong and Liu [56] identify the effect of factors like context and community factor, a transaction between buyer and seller. The issues of attacks on trust and reputation systems and their defence mechanisms are studied in [127]. The effect of credibility of ratings [56] are all trust related topics in e-commerce environments.

Multi-Agent Systems

The first computational trust model is proposed by Marsh [28] for multi-agent systems. In Marsh's model, the non-transitive and propagative properties of trust are discussed. Other popular models in multi-agent systems for managing trusts information are Bayesian systems [35, 44] and the subjective belief model [42]. In addition, Griffiths [61] provides a Multi-Dimensional Trust (MDT) model which allows agents to model the trust value of others according to their personal preference. REGRET system [70] adopts a sociological approach for computing trust in multi-agent e-commerce environment. Trust evaluation method of REGRET employs both personal and social components. Social dimension is referred as the reputation inherited by individuals from the groups the belong to. For example, when calculating the trust from agent A to agent B, we need to consider what the other members of A's group think about the agent B and B's group.

Ad-hoc Networks

Highly dynamic and distributed nature, limited information gathering ability of each peer and possibility of collusion between peers in ad-hoc networks lead to new requirements for designing trust models. The existing trust models in MANETs focus on how to model the trustworthiness of nodes and how to deliver reliable (security and privacy) packets [62, 128]. In VANETs, trust

management is not limited to reliable package delivery, i.e. building a security infrastructure [129, 130], but is also concerned with detecting false information provided by malicious peers [131].

Social Networks

Non-transitive and propagative properties of trust are hotspot issues in social networks. Golbeck et al. [39] propose trust propagation algorithms based on binary ratings. Guha et al. [49] develop a framework for both trust and distrust propagation within social networks. Hang et al. [132] propose an algebraic approach to trust propagation. They develop there operators, a concatenation operator for trust aggregation between neighbours, an aggregation operator for combining evidence, and a selection operator for multiple paths selection for social networks.

Peer-to-Peer Networks

Peer-to-Peer (P2P) networks form a major application area of trust and reputation models. The representative models include P-Grid, XREP, EigenTrust, PeerTrust and PowerTrust.

The P-Grid [133] model defines a global trust value (measured on a continuous scale from 0 to 1) to determine whether a peer is trustworthy. XREP [134] adopts a binary rating system and provide a distributed polling protocol to evaluate the reputation of each peer. EigenTrust [135] also adopts a binary rating system that computes a global reputation for each peer in a network using an algorithm similar to Google's PageRank [136]. PeerTrust [56] defines three trust metrics to measure the feedback that a peer receives from other peers, the total number of transactions that a peer performs and the credibility of the feedback sources) and two adaptive factors i.e., transaction context factor and the community context factor). Finally they aggregate these parameters into a final trust value. In PowerTrust, Zhou and Hwang [78] find a power-law distribution in a peer's feedback ratings, and develop a reputation system

PowerTrust that dynamically selects a small number of the most reputable power nodes. PowerTrust focuses on computing a global trust value.

2.2.1.2 Computational Technique-Based Taxonomy

Heuristic-Based Techniques

From the computational point of view, one type of the heuristic-based approaches is to aggregate and average quantitative feedback ratings. For example, the models in [126, 56, 61, 137, 111] calculate the summation or weighted average of ratings. At eBay, the ratings given to a seller are accumulated over a recent period and a single positive feedback rate is calculated as an indication of the seller's trustworthiness or reputation score. Xiong and Liu [56] propose a PeerTrust model which aggregate ratings to measure the trust value of a seller. Wang et al. [111] propose a RLM model, taking into account malicious ratings before aggregation. The works in [137] propose new aggregation methods taking advantage of fuzzy models, where membership functions are used to determine the trustworthiness of targets. Additionally, the concept of "flow models" is proposed in [21, 79], and "flow models" are widely used in network environments where a large number of members are involved. Essentially, they still belong to heuristic-based trust evaluation, which compute the trust of a target through some intermediate participants and the trust dependency between them. The typical ones are Google's PageRank [136] and Eigen-Trust [135]. The basic idea of PageRank [136] is to rank a web page according to how many other pages are pointing to it. To be precise, all the web pages initially have the same rank. The rank of a web page is divided evenly among its forward links, and then it will be recalculated based on its back links. Similarly, within P2P networks, Eigen-Trust [135] computes an agent trust value via multiple iterations along the trust chain until the trust values for all the agents become stable. Likewise, in social

networks, flow-based techniques are also used for trust management [49, 47, 132].

Information Theory Based Techniques

In economics, information asymmetry and reciprocity (cooperation) are two major issues of trust. The information asymmetry measured as information entropy, between trustors and trustees during interactions, can be used to measure the level of trustworthiness [8]. From the point of view of information theory, Sierra and Debenham [139,138] propose a set of metrics to measure the gap between the sellers' promises, such as product quality, and buyers' actual observations. Similarly, Adali et al. [4], in their behaviour-based social network trust model, use entropy to measure "balance in the conversation" between two network members.

Statistical Theory and Machine Learning-Based Techniques

The models in this category focus on proposing a sound mathematical model for managing or inferring trust. However, due to their high computational complexity, it becomes impractical in the environment where millions of users are to be addressed [23]. The Bayesian systems [35, 44, 140] and subjective belief models [41, 42,142, 143] are two major statistical models. The former takes binary ratings as input and computes reputation scores by statistically updating beta probability density functions (PDF), while the latter uses subjective probability theory in trust evaluation. On the other hand, machine learning techniques, such as Artificial Neutral Networks (ANNs) and Hidden Markov Models (HMMs), are adopted for trust evaluation. For example, Ham et al. [144] take advantage of RBF Neural Networks for reputation prediction in mobile ad hoc networks. In [45, 78], HMM is used for trust prediction before transactions in e-commerce environments, and ElSalamouny et al. [34], propose a discrete HMM-based trust evaluation model. In [64, 48], conditional probability model is used to infer the trust values between participants within online social networks.

2.2.2 Web service specific models

Several surveys can be found in the literature about trust and reputation in Web services [86, 84, 19]. Wang et al. proposed in [86] a classification scheme for trust and reputation systems in Web services based on three criteria:

(1) Centralized or decentralized, i.e., there exists a central party charged of managing the reputation for all the members or not;
(2) Person or resource, i.e., they target persons or resources; and
(3) Global or personalized, i.e., collected based on opinions from general population that is visible to all members or based on opinions from group of members.

In [84], the authors focuse on the trust management models and issues related to semantic Web services. They classify the trust models based on the way used to compute the trust value; resulting in three categories:

(1) Trust Computation Related to Services, where services establish trust for each other;
(2) Trust Computation on Consumer View, where consumers provide feedback on the services based on their interactions; and
(3) Trust Computation for Content and Context, which uses meta-data information to analyse the semantic data published on the Web.

In [85], the authors present a comparison summary between the reputation-based approaches proposed in the Service-Oriented Computing domain based on four criteria:

(1) Maturity: The maturity stresses the need for users' ratings when building trust.
(2) Majority: Majority points out that a certain trust mechanism should be independent from the credibility of the majority of ratings that may be dishonest.

(3) Cost: Cost refers to the complexity and extensibility of the trust mechanism
(4) Infrastructure: infrastructure refers to the ability to support distributed infrastructure such as Web services.

2.2.2.1 Single Web Service

Most of the trust and reputation models proposed for the single architecture of Web services use direct feedback collected from users to compute the trust value for the Web services. Few statistics-based, fuzzy-logic-based, and datamining-based models were proposed for this purpose.

2.2.2.1.1 Feedback-based models

Feedback-based models [87,88,89] collect reviews concerning a certain Web service in question and use them to build a trust value for the Web service. These reviews are collected from either the provider or the consumer [90]. Provider provides the descriptions of the service recorded in the service registry. Consumer-generated information is, on the other hand, online reviews provided by the users who had dealt with the service during past interactions.

Maximilien and Singh [87] proposed a multiagent framework that uses an ontology for QoS to support self-adjusting trust. By means of the ontology providers can advertise their offerings, users can state their preferences, and ratings about services can be built and shared. The ratings are based on the Web service QoS attributes such as latency and throughput but may involve also application-specific parameters such as shipping delay. The proposed framework relies on four main concepts:

- Provider quality advertisement where providers advertise their offerings of a service by specifying the minimum and maximum possible values as well as the promised values for the QoS attributes of the service.

- Customer quality preference statement where consumers describe their preferences by specifying the minimum and maximum acceptable quality thresholds as well as the preferred quality value.
- Service reputation formulation where a trust function is formulated based on the reputation function, the consumer's preferences, and the provider's advertisements. The aim of this function is to rank the services based on how well they satisfy users' requirements in order to help make selections.
- Periodic Monitoring mechanism where users are allowed to replace the poorly-performing services by other well-performing ones via a periodic monitoring of the services.

The major advantage of the feedback-based models is that the feedback provided by the consumers tends to be more realistic due to two main reasons.

- Firstly, the feedback presented by the consumers are usually user-oriented in the sense that they focus on the aspects that concern the user such as QoS and cost in contrast to the providers that tend to proclaim the service-oriented information.
- Secondly consumers have higher probability than providers of mentioning the weaknesses along with the strengths of the services.

However, this does not mean that the reviews presented by the consumers are always truthful. In fact, consumer-based reviews are usually not organized in a standardised manner in the sense that each user has his own style in writing the reviews that is different from other users (e.g.,{0, 1, 2} vs. {excellent, good, bad}). Besides, users usually tend to refrain from submitting reviews as they have no incentives for doing so, which leads to biased computation of the aggregated trust value. Most importantly, consumers are rational agents who may be tempted to provide dishonest feedback resulting in benefit for them as a result of a certain collusion scenario. For example, some consumers may collude with the providers to submit positive feedback on their services and/or negative feedback on the services of their competitors versus obtaining reduced service fees. This problem was tackled by several approaches [88,80], where the authors

consider the existence of malicious raters that may provide untrustworthy ratings. The main limitation of these approaches is that they are based on the idea that the majority of raters are credible in the sense that the rating of a certain consumer is assumed trusted if it agrees with the majority of ratings and untrusted otherwise. In this way, malicious raters can still impose their opinions and get high reputations by merely submitting a large number of fake feedback in way that allows them to form the majority.

2.2.2.1.2 Statistics-based models

These models attempt to overcome the problems of the feedback-based models by considering multiple sources of trust and using statistical methods to combine them.

In the context of single Web services, representative models [91, 92, 80] are used to compute trust values for the Web services.

In [91] the authors present a Bayesian networks based trust and reputation model for web service selection. The model fuses three sources of reputation: subjective source (direct opinion), objective source (recommendation), and conformance (between promised and actual QoS values) as follows:

$$T_x(i) = T_{dx}(i) * \omega_d + T_{rx}(i) * \omega_r + T_{cx}(i) * \omega_c$$

$T_x(i)$ is the final reputation value of web service i, in the view of consumer x. $T_{dx}(i), T_{rx}(i)$ and $T_{cx}(i)$ are direct trust, recommendation trust and conformance trust of web service i. ω_d, ω_r and ω_c are the weighting factors added to 1.

Each consumer builds a Bayesian network for each web service that it has interacted with by maintaining a set of conditional probability tables (CPT) for that web service. Each CPT is for a quality attribute of that service. Using these CPTs the values of $T_{dx}(i), T_{rx}(i)$ and $T_{cx}(i)$ can be calculated.

The advantages of the model are that

- The model allows to cover multiple aspects of QoS of a web service in trust computation.
- Consumers can specify their QoS preferences.
- Consumer can give a score for each quality attribute after each transaction.
- Evaluating the credibility of a rater based on the usefulness of the rater' feedback and the similarity between the rater and the requester.
- Using modern statistic method to calculate the probability of a hypothesis under different conditions that are equivalent to different quality attributes of the web service.

In Malik & Bouguettaya [80], authors have designed a model with reputation evaluation metrics based on real world social networks methodologies. The metrics are defined to capture most (if not all) aspects of reputation in social network that are considered essential for the accurate assessment of a provider's reputation in order to provide an effective mitigating strategy for reputation milking. We briefly describe the other metrics discussed in [80] below:

- Rater Credibility: It targets the malicious rating feedback. Not all feedback personal evaluations are honest and unbiased. A service consumer's credibility value determines the degree of trust that other consumer may have on its reported personal evaluation regarding the reputation of the Web services it has invoked.
- Majority Rating: The assessed reputation of a service provider is not a mere aggregation, but is evaluated on a majority basis.
- Past Rating History: The credibility score of a service consumer is updated based on its past rating history.
- Personal Experience for Credibility Evaluation: The consumers can evaluate the honesty of the feedback values according to the deviation between their personal experience and the personal evaluations reported by other service consumers.

- Personal Preferences: Consumers can weigh the different QoS attributes according to their own preferences.
- Personal Experience for Reputation Assessment: The 'first-hand interaction' data gets higher preference in calculating the reputation values.

A statistical technique is used to combine these metrics and compute the trust value. Given a service s, the trust value T_s is calculated as:

$$T_s = \frac{\sum_{i=1}^{L} PerEval_s^i . fd(t).C_r(i)}{\sum_{i}^{L} C_r(i)}$$

L is the set of service consumers that have invoked s. $PerEval$ is the personal evaluation value given by the consumer i. $C_r(i)$ is the creditability of i. $fd(t)$ is a function that makes the evaluation fade with time.

Experimental evidence in [80] showed that use of all the metrics together can enhance the accuracy of assessment of the reputation of a given service.

Although this is a promising approach to predict the trend of unfair ratings for evaluating the reputation of a service, they face two main drawbacks. First, detective techniques cannot produce accurate estimates of a service's reputation when the majority of raters lie. This is because statistical techniques such as collaborative filtering assume that most raters provide fair ratings and filter the false rating based on their similarity with the majority.

Therefore, if the majority of ratings are unfair, the reputation gathered from these majority samples could misrepresent one service's trustworthiness.

Therefore, these methods cannot produce reputation information correctly when dishonest raters are the majority in the community.

Second, these techniques lack sufficient ratings to foresee correctly the trend of untruthful behavior. The main reason for this is that they do not provide clear

incentive schemes to motivate raters for providing ratings to others. In general, raters are reluctant to put an effort into providing ratings to others unless they gain some benefit in return.

Finally, these models still cannot compute initial trust values for the newcomer Web services as they provide no bootstrapping mechanism that tackles this problem.

2.2.2.1.3. Fuzzy-logic-based models

In web services domain, two dimensions of reputation are (i) the subjective dimension represented by user rating of the service they directly experienced and (ii) the objective dimension represented by compliance and verity that quantify the compliance levels and their variance thereby reflecting the actual performance history.

In model [95], a fuzzy approach is used to map a relationship between these two dimensions e.g. using the objective performance measure to determine if the subjective view is rational. Technically, compliance of QoS attribute a when the service is invoked the *j*th time, is computed as

$$C_j = (a_{dj} - a_{pj}) / a_{pj}$$

a_p be projected value of a as agreed in the Service Level Agreement(SLA) and a_d be delivered value of a as obtained from the performance monitoring system.

Depending on the level of level of differentiation desired for each QoS attribute an appropriate number of fuzzy sets *viz-a-viz* membership functions are defined. For example, for three levels of compliance namely: *low*, *compliant* and *high*, membership functions "*compliance is low*", "*service is compliant*" and "*compliance is high*" are defined to map any compliance value to fuzzy equivalent.

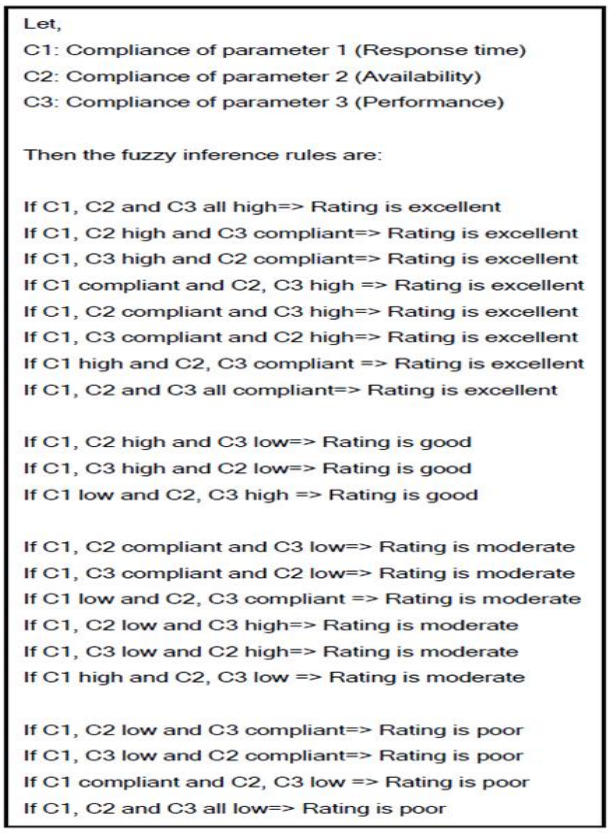

Figure 2.1: Example of Fuzzy inference rule [95]

This fuzzified accomplice value will serve as input for inference system. The output of the fuzzy inference process is the estimated rating value. Fuzzy inference rules are defined for relating inputs to the output. An example rule set is shown in the Figure 2.1. Fuzzy inference rules relate the compliance values in different attributes to an estimated rating value.

Advantage of the model is that using the inference rule, one can infer the rationale for the users' ratings. Thus explicated rationale can then be used for detecting deception, validating ratings, detecting collusion, identifying user preferences and providing recommendations to users.

Major problem of the model is that for large number of QoS attributes, a large number of inference rules will be generated.

Model [94] proposed a framework that supports a natural way of representing, querying and evaluating consumers' perception on services. A fuzzy trust data model for representing consumers' perception on QoS parameters and a fuzzy linguistic query model along with processing algorithms for the defined data model are developed. In the framework, users specify QoS requirements and preferences on various concerned QoS aspects using linguistic terms. For example, users can specify their requirements and preferences as "the service is very cheap" and "the price of the service is very important" instead of "the price of the service should be less than one dollar per day" and "the importance weighting factor of the service's price is 0.9.

Although fuzzy-logic-based models try to understand the semantic behind the ratings provided by the users, which constitutes an important topic in the context of trust and reputation, these models offer only a set of rules and comparisons as ultimate output but provide no mechanism for computing the final trust value and hence are not able to help users and/or services make selections. They cannot compute initial trust values for the new services as well. Moreover, they do not take into account the dynamism of the trust.

2.2.2.1.4. Data-mining-based models

Data mining is an interdisciplinary subject that describes the process of extracting hidden patterns from huge datasets. Data mining is becoming increasingly adopted in many domains such as medicine, engineering, science, and business. Despite its importance, this emergent discipline has not been well-exploited to address the problems related to trust and reputation in Web services. A data-mining-based approach was presented in [93], which uses the text mining to analyse the reviews provided by the users in order to evaluate the Web services and facilitate thus their selection. However, this approach is based on the naive assumption that the reviews presented by the users are always credible. Moreover, the authors didn't provide an in-depth methodology of how the text mining will be effectively performed. Additionally, the bootstrapping and trust dynamism issues are ignored in this approach.

Further steps are required leading to take advantage of the promising techniques offered by data mining (e.g., clustering, classification, frequent patterns, and association rule), and that seem to be useful to solve problems related to trust and reputation.

2.2.2.2 Composite Web services

The major goal of trust and reputation models to help composition designers select the appropriate Web services to be part of the composition process resulting in benefit for both designers (better reputation) and users (better quality). To achieve this goal, several criteria have to be taken into consideration. As composite services are no more than a set of single Web services working together to achieve a certain objective, the requirements proposed for the single architecture apply as well for the composite architecture in addition to other important requirements such as [96, 97, 98, 99,100,101]

2.2.2.2.1 Statistics-based models

In the context of composite Web services, statistical models [97, 96] have been widely used to model the relationships among the individual constituents and learn the responsibility of each constituent in the overall composite service. The objective is to help providers improve the quality of their existent compositions and make future selections. The challenges that led to the adoption of statistical models are the dynamic nature of the composite architecture and the difficulty of observing each constituent's quality. In fact, the dynamic aspect of the composition process makes it difficult to learn the order of the constituents.

Moreover, the quality of each constituent cannot be always observed. For instance, when dealing with a hotel reservation service, the user may observe sometimes that a certain constituent always responds before the others. However, such information may not be always observable. Thus, statistical

techniques are used to predict the quality of the constituents from the overall composite service's quality.

In [97], the authors employed Bayesian network to assess the trustworthiness of the constituents through a reputation-based trust mechanism. Thus, a probabilistic approach that is able to learn the composition structure of the composite services and compute the trust scores for the constituents is advanced.

Method in [96] employs the Beta Mixture [102] to assign trust for the components from the observations of the composite service. This assignment is not trivial due to the fact that (1) not all components services are visible to the consumers and (2) QoS attributes change over time. The model works in this way.

- First obtain an initial observation

  $\mathrm{x} = [\langle x_1, 1-x_1 \rangle, \langle x_2, 1-x_2 \rangle, ... \langle x_n, 1-x_n \rangle]$

  Here $\langle x_i, 1-x_i \rangle$ represents the trust value of component i in terms of number of positive and negative interactions.
- Make an initial assignment of responsibility to the components by learning the distribution $p(\mathrm{x}) = \sum_{i=1}^{n} \pi_i Beta(\mathrm{x} \mid \theta_i)$ using Expectation Maximization (EM) technique. Here $\theta_i = \langle x_i, 1-x_i \rangle$ and π_i are the observed trust and mixing weight of service component i. Once $p(\mathrm{x})$ is learned π_i is the responsibility assignment of component i
- Update the current $\theta_i = \langle x_i, 1-x_i \rangle$ and π_i for all components when the new observation x_n is collected by Bayesian inference method.

The model incorporates the dynamic nature of QoS attributes by using a discounting window.

The main disadvantage of the model is that it uses only the direct observation and indirect evidence such as referrals are not incorporated.

Although statistics-based models account for the dynamic characteristics of the QoS parameters, they cannot provide decisive solutions for this problem. In fact, these models suggest tracking the most recent behaviours of the Web services to predict their current performance.

Nonetheless, the QoS of the services may change on demand (not in an incapable of making reliable predictions. For instance, an online car rental service may face important degradation in its performance during the promotion time due to the pointedly increased number of orders. In this case, the current performance is unlikely to be predicted from the recent performance since the change in the QoS does not happen in a regular manner. Therefore, a monitoring mechanism that can capture the variations in the performance is recommended [98].

Moreover, these models ignore the collusion scenarios that may occur among the constituents of the composite service and that may lead to false estimations of these constituents' trust values. For instance, constituents may collude according to different scenarios to mislead the predictions. Additionally, statistics-based models do not study the collaboration and task allocation issues among the constituents. Furthermore, the topic of malicious constituents that join compositions to perform malicious objectives was not addressed yet.

2.2.2.2.2 Game-theoretic-based models

Game theory is a formal study of conflict and cooperation that applies whenever the actions of several agents are interdependent. Few game-theoretic-based models [100,101] were proposed to address trust and reputation in the composite architecture. The objective of these models is to model the competition among constituents seeking to get allocated with tasks in the compositions and select hence the appropriate candidate with the aim of maximizing the probability of performing the allocated tasks successfully.

As an example, Yahyaoui [100] proposed a distributed trust-based game with an objective to model the competition among services seeking to get allocated with tasks and select hence the appropriate candidate.

During the game, each Web service submits a cost for achieving a specific task. A master Web service that is allocating a specific task, computes the so-called trust-based cost, which is the product between the submitted cost and the inverse of the trust value of the bidding Web service. Trust is assessed and updated by the master Web service by using a cumulative beta distribution function. Adopting a Bayesian approach, the beta parameters are updated after each round of the game. The initial trust value (trust bootstrapping) of the bidding Web service is assigned based on its honesty during an evaluation period. The honesty is the distance between its actual quality attribute and its announced quality attribute in the Service Level Agreement (SLA).

Task allocation regulation is an important area of study in Web services composition. A proper regulation policy will increase the probability of the composite service for achieving the allocated task with better performance.

Game-theoretic-based models offer an excellent solution. However, these models do ignore some of the very important factors of the task allocation problem. More precisely, they ignore the possibility of collusion among competing services. Such collusion has an aim to promote/demote some other Web services, which may lead to inappropriate selection and create unreliable compositions.

Secondly, game-theoretic-based models can not prevent malicious constituents that join compositions to perform malicious attacks. Different from statistics-based models, game-theoretic-based models do not evaluate the responsibility of constituents in the composition process.

2.2.2.3 Communities of Web services

Communities of Web services (CWS) are formed by groups of services. Although, Web services in the communities share the same functionality, they have different non-functional properties. Formation of communities has a two-fold objective. First, the participating services will be exposed to wider groups of users and will have chances to contribute in a greater number of compositions. Second, users will get the opportunity to fulfil their request with better quality as a result of the cooperation that takes place among the services within communities.

The concept of trust and reputation is the binding force for a community to survive. Trust provides a truthful environment in a community where all members work and cooperate. To attain this truthful environment, a collection of requirements have to be satisfied. As communities are composed of single Web services and can involve some kinds of functionally-similar compositions among community members, the requirements proposed for both the single and composite architectures apply as well for the community-based architecture in addition to other important requirements such as [52,29, 31,32,53,16]:

2.2.2.3.1 Analytical models

Analytical models use mathematical models to analyse the relationships among a set of variables. These models have been used for the CWS to analyse the relationships among the reputation parameters of the Web services in order to help them decide whether to join communities or to work alone.

In [107], the authors perform an analysis on the incentives that would motivate a community (containing one or more elements) of Web services to join another community or to stay alone. They use three metrics:

- **Responsiveness Metric:** depicts the time that a community spends to answer a request. This time includes the time for selecting a Web

service from the community and the time taken by that Web service to provide the response back to user.

- **InDemand Metric:** depicts users' interests in a community in comparison to other communities.
- **Satisfaction Metric:** representing the satisfaction of a particular user with a community with regard to a service request sent the community at a given time.

Using these three metrics, they analytically establish the following three performance related functions.

- InDemand of a community during a particular time period is the ratio of the reputation value of the community to the sum of reputation of all other communities.
- Average satisfaction value of a particular user with a community in a time period monotonically decreases with inDemand of the previous period.
- Reputation of a community in a time period monotonically increases with the satisfaction during the previous period.

Based on these three functions, the authors state that a community will be encouraged to join another community if (1) it is overloaded by a huge number of requests, or (2) it is unable to attract enough services satisfying its Web services.

Their model provides the basis for a single Web services to predict their further reputation level (and thus, performance) that let them make the best decision.

However, their model restricts the reputation assessment to three metrics; thus ignoring some important factors such as capacity of handling requests.

In [103], the authors introduce a reputation mechanism to select the Web services having the best credibility based on two crucial parameters: *satisfaction* and *popularity*. They analyse the impacts that these parameters

have on one another in continuous service selection processes. Two metrics are used:

- **InDemand Metric:** measures the market share of a Web service in comparison to other community members in in terms of the proportion of user requests it receives at a time unit t .
- **Satisfaction Metric:** measures the users' satisfaction of the obtained service from a Web service at a time unit t .

A weighted mixing of these two metrics is used a measure of service reputation in the next time unit $t+1$. As all three metrics are dependent on the number of user requests (and subsequently users ratings after evaluation of received service from the Web service), in the analysis, a *non-homogeneous Poisson process* is used to model the dynamics of users requests. The arrival of request for a Web service during a time unit t is defined as

$$m(t) = \int_{1}^{t} \lambda(x)dx$$

$\lambda(x)$ is the mean number of requests at time moment in time unit t i.e., the interval $[i,t]$.

Using the mathematical treatment of this Poisson process, the authors analyse the impacts of satisfaction and popularity under two cases:

- Case 1: the Web service is overloaded with users request i.e., its market share is more than its capacity.
- Case 2: the Web service is idle i.e., its capacity exceeds its market share.

The analysis results show that Case 1 will result in a decrease in the Web service's reputation and the change in the reputation in the current time either positively or negatively leads to a negative change in the reputation in the next time unit. In the second case, the analysis revealed that a positive rate of reputation change at a certain time results in a positive rate of change in the next time slot.

Their model considers the performance of handling users and the relation between this performance and the Web services reputation. The results of the analysis can equip Web services with reasoning capabilities allowing them to decide to join community or stay alone. The reasoning technique would help the Web services to increase their overall performance in dynamic networks.

However, the analysis is limited to only two reputation factors measured by the Web service; and thus eliminating the reputation parameters related to users. Further, they restrict their discussions to honest feedback submission and thus, consider the reputation assessment accurate.

In [96], the authors develope an analytical model that analyses the incentives that would demotivate the community coordinator from behaving maliciously by either increasing its reputation level or decreasing other communities' reputation levels illegally. To tackle this issue, a third-party called agent controller is assigned the role of recognizing the misbehaviours by comparing the community's reputation change (improvement or degradation) between two slots of time and matching this change with a predefined threshold.

Likewise the previous two models, the authors in [96] also limit the analysis to three reputation metrics.

Although analytical models tend to provide strong solutions since they are based on mathematical proofs, these models fail to provide solid decision making frameworks for the Web services since they restrict the analysis to few parameters. Moreover, analytical models provide no bootstrapping mechanism to compute initial trust values for the new Web services and communities. Furthermore, they do not account for the malicious Web services that join communities to launch attacks deteriorating communities' QoS and reputations.

2.2.2.3.2 Game-theoretic-based models

Game-theoretic-based models provide in-depth reasoning mechanisms for understanding the behaviours and actions of the different agents involved in the community-based architecture. These mechanisms, as a result, are able to provide effective and powerful decision making frameworks for community members.

A one-stage game theoretical model has been developed in [105] to provide Web services with a decision making framework that helps them adopt strategies inside and outside communities. A heuristic is used for the calculation of performance as

$$E_x = \frac{R_x \times M_x}{|Rq_x - C_x| + 1}$$

Here R_x is the reputation, M_x is the market share, Rq_x is the obtained service request and C_x is the capacity.

Using the proposed game, the authors derive a threshold to be compared with the expected performance. If the expected performance exceeds the threshold, then the strategy will be joining for the single Web service and accepting the invitation to join for the community. Another threshold is derived to control the strategies of the Web services inside the communities. If the expected performance exceeds this threshold, the strategy of the single Web service would be leaving the community; otherwise it would prefer to remain.

The major contribution of this model is a decision framework for a Web service to identify the best time to join a community to cooperate with others to increase its performance. However, the framework does not consider the possible malicious nature of the services joining the communities. It assumes hence that all the parties involved in the game (coordinator, single Web services, and users) are trusted.

Khosravifar, Bentahar, Moazin, and Thiran [146] use a game-theoretic analysis to maintain accurate reputation assessment for agent-based web service systems. In this reputation assessment framework, web services are ranked using users' feedback posted with respect to the quality and satisfaction of the received service. A controller agent is responsible for supervising the feedback file against the false feedback with an aim to seize malicious acts from the community members. Failing to detect malicious acts from the community members may lead to the case of penalizing a good member by mistake (false positive) or the case of ignoring a malicious member by mistake (false negative).

The following inequality is used as a detection criterion to capture suspected behaviour of the community member.

$$\left| \frac{R_i - R_{i,\alpha}}{R_{i,\alpha}} \right| \succ \upsilon$$

R_i is the current reputation level of the web service i and $R_{i,\alpha}$ is the general assessment of the same web service reputation without considering the $1-\alpha$ percent of the recent feedback.

A two-player game is used to investigate the payoffs obtained through different situations and propose solutions that allow building collusion-resistant reputation mechanism.

The work of [146] is extended to model the collusion scenarios that occur among Web services acting as intelligent agents in [104]. The objective is to guarantee a truthful environment where involving entities act honestly. In this context, a repeated game model was derived in order to maintain sound reputation mechanism in the presence of malicious services seeking to enhance their reputations by means of fake feedback. To this end, the authors discussed

four scenarios the controller of the community (charged of monitoring the feedback file against manipulations) may face such as:

- Malicious act not penalized: This is the case where a web service that acts maliciously by colluding with some users cannot be recognised by the controller and hence the web service increases its reputation level.
- Truthful act penalised: This is the case where web service that acts normally is penalised by the controller agent.
- Truthful act not penalised: This is the ideal case where a web service acts normal and the controller refuses to penalize.
- Malicious act penalised: This is also the fair case where a web service that acts maliciously hoping to increase self-reputation level is detected and penalised by the controller agent.

Using a repeated game of two players (Web service and controller) the best strategy for both players are derived. The work analysis disclosed that if the service is made aware of the penalties that it may undergo as well as of the controller's detection accuracy, then the system would fulfil sound and secure state.

However, the system does not take care of the possibility that the controller agent who is responsible for supervising the feedback file against false feedbacks may be itself involved in the collusion between Web services and consumers.