J. Parallel Distrib. Comput. 75 (2015) 184–197

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

journal homepage: www.elsevier.com/locate/jpdc

# Reputation systems: A survey and taxonomy

Ferry Hendrikx, Kris Bubendorfer *, Ryan Chard

*School of Engineering and Computer Science, Victoria University of Wellington, New Zealand*

## HIGHLIGHTS

- The concepts for reputation systems are discussed.
- A survey of existing reputation systems is presented.
- We construct a new taxonomy for reputation systems.
- We identify under-represented areas for research.

ARTICLE INFO

*Article history:*
Received 29 July 2013
Received in revised form
2 August 2014
Accepted 17 August 2014
Available online 23 August 2014

*Keywords:*
Reputation system
Survey
Taxonomy
Feedback

ABSTRACT

In our increasingly interconnected world, the need for reputation is becoming more important as larger numbers of people and services interact online. Reputation is a tool to facilitate trust between entities, as it increases the efficiency and effectiveness of online services and communities. As most entities will not have any direct experience of other entities, they must increasingly come to rely on reputation systems. Such systems allow the prediction who is likely to be trustworthy based on feedback from past transactions. In this paper we introduce a new taxonomy for reputation systems, along with: a reference model for reputation context, a model of reputation systems, a substantial survey, and a comparison of existing reputation research and deployed reputation systems.



## 1. Introduction

Online interactions between people and services that have no prior real-world relationships are increasingly common. Examples of interactive online sites include Social Networks (e.g. Facebook [27], Crowdsourcing [39,22], Wikis (e.g. Wikipedia [92]), Forums (e.g. Stackoverflow [80]), and modern paradigms such as F2F sharing (e.g. Dropbox [24]) and the Social Cloud [12,11]. All of these interactions can be considered to include an element of reputation, such as post-counts in forums, competencies in crowdsourcing and social linkages and endorsements in social networks and the social cloud. The need for reputation systems can only, in our view, grow in importance in our increasingly interconnected world.

A reputation system works by facilitating the collection, aggregation and distribution of data about an entity, that can, in turn, be used to characterize and predict [18,67,69] that entity's future actions. In essence, by referring to reputation data, users are able to decide whom they will trust, and to what degree. In addition, the existence of a reputation system is socially corrective, as the incentive of positive reputation and the disincentive of negative reputation will generally encourage good behavior over the longer term. Once reputation data is collected, it can be shared amongst users to closely emulate some of the characteristics of a long-term relationship [66], without ever having to have previously interacted.

The requirement for trust and reputation is evident in many online systems. In online banking systems for example, the reputation of the service is implicit. In more open online business systems and electronic markets such as eBay [25], we observe the explicit yet informal use of reputation through user feedback. Building and maintaining a good reputation can be a significant motivation for contributing to online communities, be they scientific, business or socially oriented. It has been shown that a good reputation leads to more sales, at a higher value than might otherwise be possible [68]. Existing online reputation models, while diverse, are still in their infancy and are generally limited in scope, usually focusing on a single context for information. There are, in addition, valuable lessons for reputation systems that can be taken from the real world, such as credit scoring systems. These systems allow banks to rank borrowers according to "historical data and statistical techniques" [55]. A credit score is based on multiple facets such as the

* Correspondence to: School of Engineering and Computer Science, Victoria University of Wellington, PO Box 600, Wellington 6140, New Zealand.

*E-mail addresses:* ferry@ecs.vuw.ac.nz (F. Hendrikx), kris.bubendorfer@ecs.vuw.ac.nz, kris@ecs.vuw.ac.nz (K. Bubendorfer), ryan@ecs.vuw.ac.nz (R. Chard).

http://dx.doi.org/10.1016/j.jpdc.2014.08.004
0743-7315/

borrower's address, time at that address, employment, time with that employer, income, savings, family size, and loan to debt ratio [9].

### 1.1. Contributions

In this work we have surveyed numerous reputation systems built for both academic and commercial purposes, and from these derived a set of dimensions that, in our opinion, best describe the definitive aspects of reputation systems. These dimensions have then been used to construct a new reputation taxonomy using the iterative methodology described in Nickerson et al. [59]. In the construction of the taxonomy we have also developed a new reference model for reputation context and a general model for reputation systems.

A desired outcome of any taxonomy is to identify opportunities for research, and to this end we have applied our taxonomy to a large body of existing work, and through this identified a number of new or under-represented research areas. In addition, our taxonomy provides a consistent unified descriptive reputation vocabulary, and the means to define and compare reputation systems with regard to their functionalities.

### 1.2. Organization

The rest of the paper is organized as follows. In Section 2 we discuss trust and risk, followed by Section 3 in which we present models for context and interactions, and the primary survey. We then use this survey to construct the taxonomy given in Section 4. In Section 5 we present the classification of reputation systems using our taxonomy. In Section 6 we present work related to reputation system taxonomies, and this is followed by supplementary characteristics in Section 7 and finally our conclusions are given in Section 8.

## 2. Trust, risk and reputation

While reputation is the main concern for this paper, the concepts of trust and risk are important considerations. Reputation and trust (or trustworthiness) are commonly confused [56] and used as synonyms, even though their meanings are distinctly different.

According to the Collins English Dictionary, reputation is *"the estimation in which a person or thing is generally held; opinion"*. Every person's opinion differs from every other person, making reputation a highly personal and subjective quantity [70]. Reputation is not what character someone has, but rather what character others think someone has. For this paper we will use the definition of reputation created by Mui et al. [57] *"the perception that an agent creates through past actions about its intentions and norms"*.

Jøsang et al. [42] define trust as *"the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible"*. The key concepts in this definition are dependence and reliability; these values are measured, in part, through a person's reputation. It can therefore be said that trust can be established through the use of reputation. Arguably, a better reputation can lead to greater trust.

Risk is often undertaken in the hope of some gain or benefit. Risk can therefore be viewed as the situation where the outcome of a transaction is important to a party, however the probability of failure is non-zero [42]. Incorporating our previous notion of trust into this definition: the amount of risk that a party may be willing to tolerate is directly proportional to the amount of trust that the party has in the other party.

The main aim of reputation systems is therefore to support the establishment of trust between unfamiliar parties. Dellarocas [17] states that the aim of eBay's feedback mechanism, and in a generalized sense, all reputation systems, is to "generate sufficient trust among buyers to persuade them to assume the risk of transacting with complete strangers". Despotovic and Aberer [18] talk about "reducing the opportunism" and vulnerability of the two parties. Using a reputation system, a party may examine the history of another and decide that it will trust and interact with the other party. This decision is often called a "trust decision" [47].

## 3. A brief survey of reputation systems

In this section we present a survey of a number of reputation systems that were core in defining the dimensions of our taxonomy. However, in order to present these systems in a consistent and meaningful way, we must first present two reference models we have developed. The first reference model is needed to unify the description of reputation context, the second to describe the system model.

### 3.1. A reference model for reputation context

Reputation is context dependent and relies on contextual information to give data meaning [3]. The definition of context with respect to reputation systems is often difficult to determine and there is no common definition used by researchers.

Reputation systems are often discussed as utilizing additional contextual dimensions [71], facets [31], or attributes [13] to provide greater meaning and usability to the information generated during a transaction. In order to unify this concept we have adopted the term contextual attributes. Contextual attributes are like metadata, in that they help to describe the transaction in greater detail. For example, the date, the price, the buyer and the seller are all possible attributes of a transaction between two parties.

Contextual attributes however, are not the entire picture. For that, we require a context, which is the domain in which the information was generated. Most reputation systems employ a single, or personal, context. In other words, most systems consider only the reputation of an entity in the "function" of the system (whether that be e-commerce, expert advice, or file sharing).

Reputation systems employing more than one context often add additional domains of information. For example, the addition of a social context to an existing personal reputation context can help to determine if an individual contributes to his or community and therefore if they are more trustworthy.

In an effort to summarize and clarify the relationship between context and reputation, we have developed a reference model based on a psychological framework of personal identity [82]. Our reference model is presented in Fig. 1. Starting with the innermost ring, reputation context can be personal (who), professional (what), organizational (which/membership) and societal (where).

Most online reputation systems focus only on the personal reputation of a person, whilst many real-world situations deal with non-personal aspects, such as a user's professional and organizational membership.

### 3.2. A reference model for reputation systems

When discussing reputations systems, it is important to define the parties involved and their potential interactions. In Fig. 2 we present our generalized model of reputation systems that we have designed to accommodate both real-world and online approaches to reputation.

The Trustor is a party that wants to trust and interact with a target entity, called the Trustee [18,47]. In order to make a

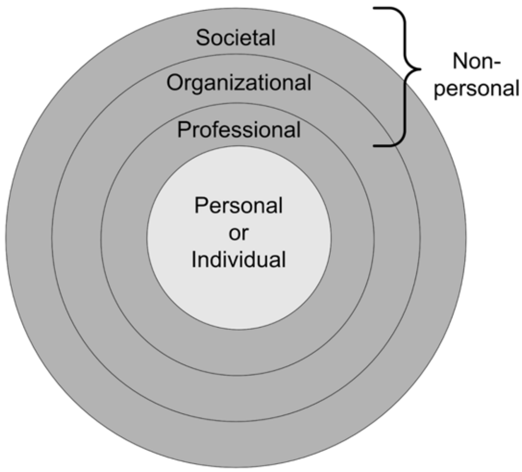



**Fig. 1.** A reference model for reputation context.

trust decision about whether to trust the Trustee, the Trustor will need to evaluate the Trustee's reputation [48]. It does this by first consulting its own internal reputation information, to see if it has previously interacted with the Trustee and what the outcome was. However, if there was not any previous interaction, the Trustor will then query $1..n$ Recommenders [72,69,47,51] that may have previously interacted or observed an interaction with the Trustee for their opinions.

A Recommender may be an entity that provides information from its own history of transactions, or a system that either observed an interaction between two parties, or collects information from other sources [51]. A Recommender with appropriate information may reply with a recommendation (also called feedback or rating in this paper). A Recommender may have a variety of first and third hand information; this is represented by the $1 : 0..n$ relationship between the Recommender and its internal reputation information.

Using the reputation information obtained from the Recommenders, the Trustor is able to make its trust decision. The roles of Trustor, Trustee and Recommender are interchangeable [47]; if the transaction proceeds, both parties will have their own reputation information that may subsequently be made available to other parties making similar decisions.

### 3.3. Survey of academic reputation systems

The **Regret** [73,71] reputation system is designed to operate within an electronic marketplace setting. The system utilizes multiple contextual attributes and classifies information as coming from an individual, social, or an ontological dimension. The individual dimension considers information directly gathered from interactions between two entities. The information is fine grained and often relates to the frequency of overcharging, late delivery and quality of the transaction. The social dimension is an addition to the Regret system, where trust can be extracted from the groups and communities associated with the target entity. A key benefit of the social dimension is that it allows new and unproven entities to bootstrap their trustworthiness by belonging to reputable groups. Alternatively, because the entire group's reputation is associated with the behavior of its members, it is pertinent for a group's members to moderate the behavior of those associated with them.

The work also includes an ontological dimension, where reputation collected for atomic aspects are combined to construct more complex graph structures in order to derive further insight. Ratings, or impressions, are recorded as a value between positive and negative one. An entity's reputation is then the aggregation of the result of all transactions they have taken part in. When utilizing the ontological dimension, each atomic aspect is calculated using individual and social dimensions, and then combined through a weighted graph for more complex evaluation. The computation of the ontological reputation, $OR_{ij}$ is achieved through Eq. (1). Where each child in the graph is computed with a weight $w_{xy}$ to establish a score. An example of this computation can be seen in Eq. (2) where the social dimension $SR_{ij}$ for each aspect is weighted and used. The Regret system also employs a degree of reputation decay, called a forget factor, where only the most recent transactions are considered.

$$OR_{ij}(x) = \sum_{y \in children(x)} w_{xy} OR_{ij}(y) \tag{1}$$

$$\begin{aligned} OR_{ij}(good\_seller) = \; & 0.2 \times SR_{ij}(delivery\_date) \\ & + 0.2 \times SR_{ij}(product\_price) \\ & + 0.6 \times SR_{ij}(product\_quality). \end{aligned} \tag{2}$$

**Confidant** [8] incorporates a reputation system into a Dynamic Source Routing protocol in mobile ad hoc networks. The Confidant protocol is a structured system designed to identify and isolate

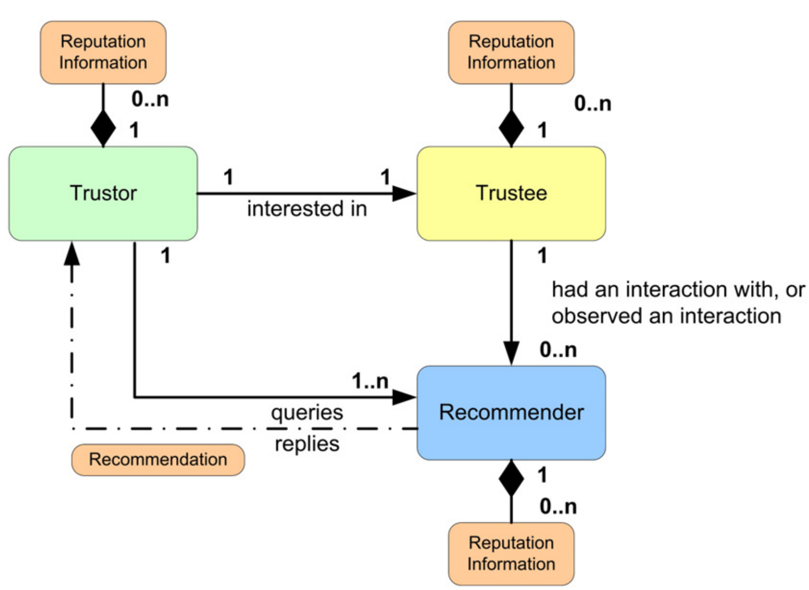



**Fig. 2.** A reference model for reputation systems.

misbehaving nodes in the network. The system allows entities to monitor the behavior of others, regarding their ability to manipulate information and correctly route, forward and participate in the protocol. Nodes are inherently trusted and malicious behavior is reported, resulting in a form of punishment.

An alarm message is generated when a node experiences, observes or receives a report of malicious behavior. Observed information is gathered by examining the interactions among neighbors. Alarm messages are then passed on to other nodes in the network to warn them of the misbehaving node. When an alarm message is received from another entity, their trustworthiness is considered before passing the alarm on. Ratings are stored as local lists and black lists at each node, and are potentially shared with friends. Confidant proposes to lessen the effect of false accusations with a reputation death property and revocation lists, meaning entities are capable of redeeming themselves over time as historic actions are removed from the system. No specific aggregation equations are published.

**XRep** [16] is an extension to GNUtella-like peer-to-peer (P2P) networks. XRep allows for the creation and maintenance of reputation for both resources and nodes in the network. Each node maintains a personal history for both resources and nodes. For resources, a simple binary rating is used, while for nodes a count of the number of successful and unsuccessful downloads is maintained. Reputation messages are piggybacked on existing connections and allow nodes to select resources based on criteria other than purely resource based. When deciding where to download a resource, a node first contacts its peers for their advice (using a poll operation), and then evaluates the responses. Once the node has selected the appropriate resource, it can evaluate potential nodes that offer the resource and select one based on reputation. Assigning reputation ratings to both resources and nodes in the network gives XRep a number of advantages. These include judging new resources by the nodes offering them, load balancing using a resource reputation rather than purely the node reputation and whitewashing avoidance as changing pseudonyms removes nodes from being selected. A set of extensions to XRep, called X$^2$Rep [15] were created later and addressed some of the weaknesses in XRep.

**EigenTrust** [44] is a peer-to-peer (P2P) reputation framework that allows entities to decide which others they will trust when it comes to downloading files. It is fully decentralized, and utilizes a distributed hash table overlay. Each entity maintains a personal history for other peers, which is simply the sum of positive and negative interactions they have experienced with them. These values are normalized between 0 and 1. An entity calculates the global Trust for another entity, $T_{ij}$, by using personal histories which are obtained from others in the network. These histories are weighed by the credibility of the reporting entity, as seen in Eq. (3), where $e_{ix}$ denotes a local trust value of entity $i$ for entity $x$. In essence, the system uses the direct experience of others and a local perception of the reporting peer to compute trust [37]. To compute trust in a distributed environment, the aggregation model represented by Eq. (4) is used. This is a component-wise method of computing the global trust of $i$ which aggregates the trust each peer holds in $i$ over a time period $k$. Where $\alpha$ is a constant less than 1 and $p$ is used to add trust to new entities in the network.

$$T_{ij} = \sum_k e_{ix} e_{xj} \tag{3}$$

$$T_i^{(k+1)} = (1-\alpha)(e_{1i} T_1^{(k)} + \cdots + e_{ni} T_n^{(k)}) + \alpha p_i. \tag{4}$$

**P-Grid** [3] is a peer-to-peer (P2P) platform for distributed information management. P-Grid is completely decentralized and self-organizing. Information is spread across the environment among peers via a distributed search tree, similarly structured to distributed hash tables. As is the case with Confidant, entities in P-Grid are considered inherently trustworthy, and only malicious behavior is deemed relevant. Entities are able to forward complaints about transactions to others within the environment. These complaints are distributed in the form of messages to arbitrary entities. P-Grid implements a binary trust model, where entities are either trustworthy or not. When an entity wishes to evaluate the trustworthiness of a target, it performs a search for complaints. These are fed into a trust function such as that shown in Eq. (5). The function is used to determine whether $i$ can trust the entity $j$. Where $Cr$ denotes complaints received and $Cf$ represents complaints filed. $Cr_i^{avg}$ and $Cf_i^{avg}$ are the aggregate of all observations the entity $i$ has made over its lifetime. If the equation computes as true, then the entity is considered trustworthy, otherwise they are not.

$$Cr_x^{norm}(j) Cf_x^{norm}(j) \leq \left( \frac{1}{2} + \frac{4}{\sqrt{Cr_i^{avg} Cf_i^{avg}}} \right)^2 Cr_i^{avg} Cf_i^{avg}. \tag{5}$$

**PeerTrust** [94] uses a structured peer-to-peer (P2P) overlay network to host a distributed implementation of their transaction-based feedback system. The simulation used to demonstrate PeerTrust utilizes P-Grid to distribute feedback scores. The system incorporates a combination of fundamental reputation sources, such as direct feedback, and the quantity of transactions performed, while weighting feedback with credibility. The work introduces two novel trust metrics, a community context factor and transaction context factor. The simulation presented in the work has entities generate a rating of either zero or one.

The trust of an entity $i$ is computed by Eq. (6). Given $N_i$ is the total number of transactions entity $i$ has taken part in. $P_{ij}$ denotes the other entity involved in the transaction. $S_{ij}$ is the normalized level of satisfaction $i$ received from peer $P_{ij}$ from the transaction. $Cr$ denotes the credibility of the feedback received from the entity $P_{ij}$. $TF_{ij}$ represents the adaptive transaction context factor for entity $i$'s $j$th transaction, and $CF$ denotes the community context factor for $i$ during a period of time. The normalized weighted factors $\alpha$ and $\beta$ are the collective evaluation and the community context factors, respectively.

$$T_i = \alpha \sum_{j=1}^{N_i} S_{ij} Cr(P_{ij}) TF_{ij} + \beta CF(i). \tag{6}$$

**RateWeb** [52] is designed to facilitate trust between Web services. RateWeb utilizes a decentralized and unstructured approach. The system's goal is to provide a method in which Web services can reliably be used as independent components in a service-oriented enterprise without the intervention of humans.

When selecting a Web service to accomplish a task, the consuming entity queries the community for a list of suitable services. A set of eligible Web services are then returned to the consumer. The response also includes a list of past consumers that possess feedback for each service. Rather than acting as a centralized repository of feedback, the community acts as a directory of raters. Each entity stores a personal perception of each Web service it has invoked. The feedback is stored in a vector of values that represent the promised quality against the delivered quality of an attribute.

The reputation of a service $s_i$ can be computed by an inquiring consumer through Eq. (7). Where $L$ denotes the set of consumers which have interacted with, and rated, the service $s_i$. $PerEval^x{}_i$ represents the personal perception a consuming entity has of the service $s_i$. The credibility $Cr_x$ of each consuming entity, as viewed by the inquiring consumer, is within the interval [0, 1]. A reputation fader, or decay factor, $D_f$, is also incorporated and is a value within [0, 1].

$$Reputation_{s_i} = \frac{\sum_{x=1}^{L} [PerEval^x{}_i D_f C_r(x)]}{\sum_{x=1}^{L} C_r(x)}. \tag{7}$$

A credibility-based model is also included within the framework. In this model, each service contains a set of trusted entities to query when requesting ratings. If none of the group contain experience with the entity in question, each group member can refer the request to their own trusted set of entities.

**R$^2$ Trust** [84] is a fully distributed reputation system for large-scale, decentralized overlay networks. The system is designed to incorporate reputation and risk to provide trust within an unstructured network. The reputation of an entity in the network is calculated by examining any direct interactions an entity may have had and obtaining recommendations from other peers. Recommendations are weighted using local trust values for the originating peers. The trust value assigned to any given peer is built using social relationships and considers the risk inherent in those relationships. This allows the framework to react quickly when the behavior of a given peer changes. R$^2$Trust determines quality of service as probabilistic ratings between zero and one. These values are then aggregated and accumulated to give an entity a reputation value. In order to filter out untrustworthy second-hand opinions, a credibility score is used to weight feedback during aggregation. A decayed trust value, $DT_{ij}$ reduces the significance of feedback over periods of time, as shown in Eq. (8). Where $\lambda_k = p^{n-k}$ is the decay factor of time period $k$, and $0 < \lambda_k < \lambda_{k+1} \leq 1, 1 \leq k < n$. $e_{ij}^{t_k}$ denotes a local trust value of entity $i$ for entity $j$ over the time period $t_k$.

$$DT_{ij} = \frac{\sum_{k=1}^{n} (\lambda_k e_{ij}^{t_k})}{\sum_{k=1}^{n} \lambda_k}. \tag{8}$$

**GRAft** [33,34] (Generalized Recommendation Framework) is a distributed reputation framework built on the Kademlia DHT. Reputation information is collected from diverse online sources to form recommendations. These sources can be explicit reputation information such as ratings and scores (e.g. Karma or H-index [36] scores), or implicit information such as the number of connections in a social network. Reputation information for each GRAft registered entity is both stored, and distributed, using profiles. The XML-based profile stores each entity's reputation information in a string format, allowing the profile to maintain the information in the original source format. GRAft does not aggregate or process this reputation information in any way, allowing a subsequent requestor to decide how the information should be used and judged. Instead, GRAft agents use policies to make decisions about entities. For example, in a professional collaborative setting, Eq. (9) describes *Co-authors, and Co-authors of co-authors, that are employed by either Acme Corporation or Studentville University* [34], where $t$ represents the trustee, $c$ the degree of co-authorship from the trustee to the trustor, and sets $A$ and $U$ represent Acme Corporation and Studentville University respectively. This policy can be used by a resource owner to limit access to a loosely defined set of individuals.

$$(c \leq 3) \wedge ((t \in A) \vee (t \in U)). \tag{9}$$

### 3.4. Survey of commercial reputation systems

**Amazon** [6] allows its registered users to write reviews on products. A user must first buy a product from Amazon, however they may then review any product carried by Amazon using a numeric rank (5 stars). Another Amazon user may then leave a boolean feedback rating of either "helpful" or "not helpful" for a product review. Reviews may be ordered by the number of "helpful" votes they have received. The reputation of a review author rises with each 'helpful' vote [51]. Amazon maintains a ranked list of reviewers based on their reputation, allowing them to apply badges such as "top 10 reviewer" and "top 500 reviewer" to their reviewers.

When considering online reputation systems, **eBay** is both well researched and much written about [66,68,67,38,54]. eBay is an online auction site, allowing sellers and buyers to trade goods through an auction process. At the end of a transaction, both parties to the exchange leave feedback for each other. This allows potential future parties to examine the reliability of any target party that has had a previous interaction. Feedback is left in the form of a single overall rating (Good, Neutral and Negative), a series of numerical ratings (for the following facets: Accuracy, Communication, Shipping Time and Shipping Charges) and a comment. The comment often provides further information about the actual quality of the item, shipping or any problems encountered.

**Epinions** [26] is a consumer products review site, founded in 1999. Users do not have to purchase anything and may write reviews on any product they chose, although they are encouraged to focus on new or previously unreviewed products. Good reviews can earn royalties on sales of the product that was the subject of the review.

Users do not have any visible reputation rating, however badges such as "top reviewer" and "popular author" are assigned to active users with good review ratings. Users are however able to maintain a list of other users that they trust. The number of users that trust a given user is publicly displayed, and acts as a form of reputation.

**Slashdot** [77] is a technology news website, founded in 1997. It is one of the earlier sites to utilize a reputation system. All registered users have an amount of "karma" that changes over time to reflect their level of activity, which includes the posting of articles and commenting. Users with a good level of karma are able to become comment moderators [63].

**Stackoverflow** [80] is a dedicated Question and Answer site for developers, both "professional and enthusiast". Users post questions that may then be answered by other users. Reputation points are awarded for all tasks (including asking and answering questions). However, more points are awarded for comprehensive answers as chosen by other users. As a user gains more points, they are able to access further features on the site, including the ability to vote up, vote down and act as a moderator (i.e. edit other user's questions and answers). A user that votes down a particular answer will lose 1 reputation point. Presumably this is intended to stop users from voting down too much.

Each user has a profile that features their reputation score, and how they achieved that score. The reputation score is represented using a discrete value; the more reputation points a user has, the higher their score.

**Turkopticon** [89] is an third-party reputation system for crowdsourced workers using Amazon's Mechanical Turk (AMT). It allows workers to check the reputation of work providers when viewing potential jobs. In particular, it allows a worker to view and rate a work provider on 4 facets of their behavior (Communicativity, Generosity, Fairness and Promptness).

Turkopticon is integrated into a worker's experience of AMT using a browser plugin. The plugin inserts the rating information into the AMT pages as they are rendered on the user's browser. Rating information is centrally maintained by Turkopticon, and maintained using worker input. Regular software updates improve the worker experience and resolve technical issues.

## 4. A taxonomy for reputation systems

### 4.1. Taxonomy construction methodology

We have applied an iterative approach of taxonomy construction, as described Nickerson et al. [59], where both an "empirical to deductive" and "deductive to empirical" approach are used. In this overall approach, the primary purpose of the taxonomy is used to drive the identification of the key dimensions and their characteristics. Given that the purpose of our taxonomy was to contrast and compare the architecture, organization and management of different reputation systems, our key dimensions focus on the structure, design and organization of these systems. We examined the dimensions in existing commercial and research reputation systems, and included those that related to our chosen dimensions. We then added further dimensions that are important as regards reputation systems architecture, organization and management. Our dimensions and characteristics were then used to classify a diverse set of reputation systems. This allowed us to refine our dimensions and characteristics by ensuring they could fully describe this set. We then independently classified a number of other reputation systems, and compared the results of the classification. These were used to identify the dimensions and characteristics that required further work or were not defined clearly enough. This process was repeated until no further changes were required.

### 4.2. The taxonomy

Our reputation taxonomy is given in Fig. 3. The first level of the taxonomy distinguishes between explicit and implicit reputation systems. An implicit reputation mechanism represents systems that have not defined a reputation system, however reputation information is still employed by its members to assist in making decisions. The oldest and simplest form of implicit reputation system is the social word of mouth system as discussed by Dellarocas [17]. These "systems" have little or no structure, and have been used for centuries to ensure that participants in transactions remain honest, even when faced with the temptation to cheat the other party for short-term gains.

In more recent times, we can find examples of implicit reputation systems in social networks such as Facebook or LinkedIn [50]. Entities within a social network can extract some degree of trust for the information gathered through friends of friends. Although neither Facebook nor LinkedIn directly implement a reputation system, members of both systems are able to utilize reputable connections through friends within the environment. Another well-known implicit reputation system can be demonstrated in Google's [32] search engine. The order of the search results represents a ranking of pages, based on the reputation of each page. The reputation is determined by the number of links that point at the page, and where the links originate. A link originating at a page with a high reputation is likely to mean that the target page has some value. Pujol et al. [64], discuss utilizing a similar kind of topology analysis in social networks to determine reputation.

Explicit reputation systems are those that have been purposely implemented to facilitate estimation of trust between members of an environment. An explicit reputation system is typically used within an environment that relies on frequent interaction with a sufficiently sized, diverse set of members.

The second level of the taxonomy details the core dimensions of our taxonomy. The first five of these dimensions represent those aspects of reputation systems that are most often discussed in the literature:

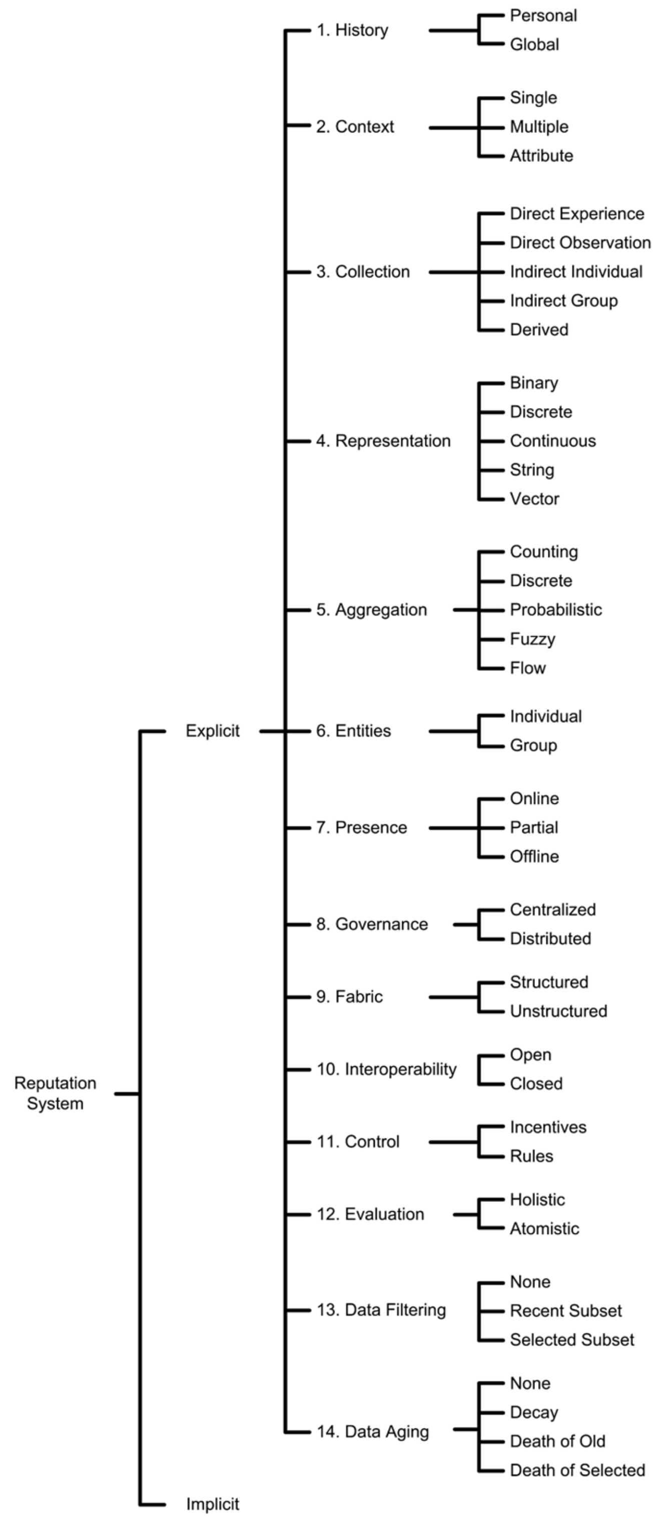



**Fig. 3.** A visual representation of the taxonomy.

#### 4.2.1. Common dimensions

1. **History**.

   A user's history is the set of stored information recording their past interactions and their outcomes. It is often used to determine the likely outcome of current, or future transactions, and is therefore central to the concept of reputation. A past transaction is often recorded in the form of an exchange between two entities, where each entity leaves feedback about the performance of the other in executing their duties and obligations. This feedback is often called a rating.

   - Personal: personal history is created and maintained using directly collected or observed information, leading to personal views of other entities. The subjective nature of these views means that others in the system may disagree with these views. This is sometimes also called localized or subjective history.

- Global: global history is created and maintained from information shared by other members in a system, leading to a consistent, global view of every entity in the system.

Further discussion on these terms can be found in Mui et al. [56], Casare and Sichman [10], Sabater and Sierra [72], Koutrouli and Tsalgatidou [48], Wang and Vassileva [91], Marti and Garcia-Molina [53] and Zhao and Li [100].

2. **Context**.

Contextual information can give a lot of meaning to data by describing a range of details regarding how interactions take place [20]. In Section 3.1, we proposed that context refer to the domain from which information is generated. In order to discuss and categorize reputation systems that utilize fine grained and transaction specific, contextual information, we adopt the term contextual attributes.

Employing this definition, the majority of reputation systems can be classified as operating within a single context, as few systems employ information from distinct domains. However, contextual attributes are frequently used to give additional meaning to transactions and can greatly increase the usability of reputation information. Schlosser et al. [74] discuss contextual attributes when providing an example of goods being sold. They explain that not only the price and quality of an item are important when buying an item, but other information such as the delivery time and after sales services should also be considered.

In addition to a typical feedback score in which a peer's behavior in a network is analyzed, Gupta et al. [31] include an explicit capability attribute when building a peer's reputation. Peers that provide desired resources to the network, such as, computing time, are given a greater supplementary reputation than those that provide few or no resources.

Reputation information can be generated from a vast number of transaction instances which are each accompanied by a significant amount of contextual information. We have categorized reputation systems as either incorporating information from a single or multiple contexts as well as maintaining contextual attributes.

- Single: a single context is assumed or maintained within the system.
- Multiple: one or more contexts is maintained within the system. Support for multiple contexts is discussed by Bagheri and Ghorbani [7], Tavakolifard et al. [83] and Grinshpoun et al. [29].
- Attribute: Contextual attributes are maintained by the system. This property is sometimes called multi-faceted, dimensional, or attribute-based, and is further discussed by Gupta et al. [31], Sabater and Sierra [71], and Conner et al. [13].

Further general discussion on context can be found in Sabater and Sierra [72], Koutrouli and Tsalgatidou [48] and Wang and Vassileva [91].

3. **Collection**.

For a reputation system to establish trust the behavioral information of entities needs to be captured. There are a number of techniques a reputation system can offer to enable the collection of information on interactions between entities.

- Direct: information is generated explicitly either from an individual's personal interactions, or observation of other's transactions. This term is further discussed in Sabater and Sierra [72] and Mui et al. [56].
- Indirect: information is obtained from other entities (either individuals or groups) based on transactions that the querying entity was not privy to. This is sometimes called witness information. This term is further discussed in Sabater and Sierra [72] and Mui et al. [56].
- Derived: information is obtained from a source that was not explicitly designed to be used as a reputation source in the current context. GRAft [33,34] derives information from non-explicit reputation sources.

4. **Representation**.

The format employed to describe, exchange and interpret reputation information. After investigating a number of frameworks and the method used to symbolize the information to members, the commonly used types of information are:

- Binary: information is stored using boolean values. This term is discussed by Kinateder and Rothermel [46], Sabater and Sierra [72], Hoffman et al. [37].
- Discrete: information is stored using discrete integer values. This term was also used by Hoffman et al. [37].
- Continuous: information is stored as a floating point number. This term is discussed by Sabater and Sierra [72] and Hoffman et al. [37].
- String: information is stored in textual form, allowing a wide range of data to be maintained. This term was also used by Kinateder and Rothermel [46] and Conner et al. [13].
- Vector: information that is either provided by multiple sources or is explicitly separated for individual use. This term is discussed by Koutrouli and Tsalgatidou [48].

5. **Aggregation**.

Aggregation describes how a reputation score for an entity is computed. The simplest form of reputation aggregation is the summation of all of the positive and negative ratings for an entity [42]. Each positive rating adds one to the sum, while each negative rating subtracts one. The final rating can be used to rank all the entities in a system. A slightly improved approach is to average all of the ratings to produce a single rating for each entity. Averaging is often used in conjunction with normalization to evaluate entities on a specific scale. Weighting the ratings by factors such as, age, reputation of the source or importance of a transaction, can provide further ways to enhance this approach. Summation, averaging, weighting and normalization are common aggregation methods and fall into a single class of simple computation called counting.

A different approach is to consider reputation as multiple discrete values as opposed to continuous values. Abdul-Rahman and Hailes [1] present a model where an entity is judged to be either "Very Trustworthy, Trustworthy, Untrustworthy and Very Untrustworthy". This is simpler for humans to work with [42], but is not optimal during computation, as the discrete rating values must be converted using look-up tables, weighted and converted back to discrete values.

Another class of aggregation involves fitting prior knowledge about another entity into a probability model and computing the likelihood of a hypothesis being correct. The hypothesis often takes the form of "is entity x trustworthy?". In other words, knowledge of prior events is used to predict future outcomes.

Aggregation using fuzzy logic is discussed by Song et al. [78]. In their system, fuzzy rules are used to determine the reputation score for both buyers and sellers.

- Counting: reputation is computed by either summing positive and negative ratings, or averaging ratings. The ratings may be weighted to provide a bias toward, for example, recent ratings or those from more reputable sources. This term was also used by Yao et al. [97].
- Discrete: reputation is computed by converting discrete rating values using look-up tables. This term is also present in Jøsang et al. [42].
- Probabilistic: ratings are fitted into a probability model and used to predict the likelihood of a hypothesis being correct. This term is discussed by Ruohomaa et al. [69], Koutrouli and Tsalgatidou [48], Hoffman et al. [37] and Yao et al. [97].

- Fuzzy: fuzzy logic is used to process or compute ratings, allowing these systems to work with a degree of uncertainty. Jøsang et al. [42] and Yao et al. [97] use this term.
- Flow: reputation is computed by examining the flow of transitive trust. This term was also used by Jøsang et al. [42] and Yao et al. [97].

Good general discussions on Aggregation can be found in Jøsang et al. [42], Hoffman et al. [37] and Yao et al. [97]. Discussions on preserving privacy during reputation aggregation can be found in Pavlov et al. [62], Steinbrecher [81] and Gudes et al. [30].

#### *4.2.2. Uncommon dimensions*

In addition to the five common dimensions already presented, we have identified further aspects of reputation systems that are not widely discussed in the existing literature. We have captured each of these aspects as dimensions in our taxonomy and each has been investigated and discussed below:

6. **Entities**.

   Entities are the primary focus, or target of a reputation system. The targets of a reputation system are typically either people or resources (for example, books or films) [91]. However, with the expansion of reputation systems there are now websites that need to cater to both. For example, Amazon allows members to rate both reviewers and resources, and Damiani et al. [16] talk about combining peer and resource reputations in peer-to-peer networks. Both people and resources are typical first class members of a reputation system. They have some similar reputational requirements, and are therefore not considered distinguishing factors in this taxonomy. Mui et al. [56] presents a reputation typology that includes the notion of "individual and group reputation". Reputation can be collected and accrued for these two different types of entities. The entities category has been included to provide a basis to differentiate between systems that operate on individuals and those that function over groups of entities.

   - Individual: these systems are focused on people or specific resources. This concept is further discussed in Wang and Vassileva [91].
   - Group: these systems are focused on groups rather than individuals. Groups can be both formal and informal in nature, with the former assuming some of the characteristics of an organization. Systems that utilize groups are discussed by Mui et al. [56], Gal-Oz et al. [28] and Tong and Zhang [85].

7. **Presence**.

   Presence describes how closely a reputation is tied to its underlying reputation system. In most early reputation systems, an entity's reputation information was only available to be fetched or updated by a central server. Later systems distributed the reputation information, however the entity holding the information is still required to be online.

   - Online: those systems that require the continuous presence of authority in order to be able to distribute reputation information. This is the default position for most reputation systems.
   - Partial: those systems that do not require the continuous presence of authority in order to be able to distribute reputation information. Initial discussions can be found in Ismail et al. [40] and Prashant and Dasgupta [19].
   - Offline: those systems that do not require the presence of authority in order to be able to distribute reputation information. This is a logical extension to the other categories in this dimension. However, we are not yet aware of any systems that could be classified as offline.

8. **Governance**.

   Reputation systems are volatile environments with entities and information changing frequently. In order for the system to function properly, providing trust within a community, some level of authority is required. Governance describes that authority, and in particular, how the system is controlled.

   - Centralized: a centralized group or organization manages the system. Most commercial reputation systems exhibit centralized governance, including Amazon, eBay and ePinions. In each instance, the underlying architecture may well be distributed, but the management is most likely by a single organization.
   - Distributed: multiple entities working together, often with no centralized management. Entities within such a system may come and go as they please. Most recent Peer-to-Peer systems display distributed governance.

9. **Fabric**.

   Fabric describes how the nodes of the reputation system are organized. The organization of a reputation system is a fundamental attribute, allowing systems to be easily categorized and differentiated between.

   - Structured: new nodes are assigned a location and a set of neighbors in an organized fashion when connecting to a network [53]. The topology may be formed using an overlay and therefore unrelated to the underlying network [75].
   - Unstructured: networks do not exhibit any organized arrangement and generally allow new nodes to connect randomly [53].

10. **Interoperability**.

    Interoperability describes the underlying principles by which the system operates and shares information. At present, most commercial reputation systems are tightly controlled and the information contained within them is not shared with third parties. This is because they consider their reputation information to be commercial property. As a result, members with good reputations are typically reluctant to leave and build up a new reputation with another provider.

    - Open: entities may freely access and utilize the reputation information contained within a system using data standards or APIs. Most academic systems fall into this category.
    - Closed: reputation information is proprietary and not usually shared outside of a system. Most commercial systems would fall into this category.

11. **Control**.

    Control describes the manner in which a reputation system motivates and controls entities to act in a desired manner, and is a fundamental aspect of any implementation. Arguably reputation systems are themselves are socially corrective, however this dimension is only concerned with explicit rules and incentives/disincentives used within a reputation system in order to get entities to behave in the desired manner.

    - Rules: an entity is forced or limited to act only within a prescribed manner.
    - Incentives/Disincentives: an entity is motivated or guided using rewards and punishments to obtain appropriate behaviors. Incentives are further discussed in Jurca and Faltings [43], Wongrujira and Seneviratne [93] and Marti and Garcia-Molina [53].

12. **Evaluation**.

    When obtaining or viewing the available reputation information for a given target entity (the trustee), reputation systems may provide two different views of previous transactions.

- Atomistic: a detailed transaction-based view that potentially shows all of the interactions that the trustee has had. This can be used to window-in on only one aspect of the available reputation information.
- Holistic: all of an entity's interactions are considered and weighed to provide a single, overall view of the trustee to the trustor. No detailed information is provided, only the summarized information is available for evaluation.

13. **Data Filtering**.
    - None: data provided by the system is not limited or filtered in any way. Trustors may utilize the full available history for a given trustee.
    - Subset: data provided by the system is limited by the application of data filtering. Trustors may utilize only a subset of all available history for a given trustee. A subset is most usually based on the age of the data, or some manual selection.
14. **Data Aging**.

    Data Aging essentially reduces the confidence of information as time passes and more information is collected. The decay in value of information allows entities to distance themselves from historic behavior. Information decay helps prevent attacks on the reputation system in which entities build a sufficient level of trust and then begin acting maliciously. As the most recently gathered information is given the largest weight of confidence, new negative behavior will have the largest impact when making decisions.
    - None: reputation information is retained indefinitely.
    - Decay: reduces the confidence and granularity of older reputation information as time passes. Koutrouli and Tsalgatidou [48] discuss this idea further.
    - Death: an extension of decay that allows older reputation information to be discarded [99]. Information is usually discarded based on age, or a manual selection.

## 5. Classification of reputations systems

In this section we apply our reputation taxonomy to classify a large number of academic and commercial reputation systems, see Tables 1 and 2. In these tables a '?' in a cell indicates that information on the characteristic was not available in published work. Multiple entries in a cell indicate that multiple characteristics are supported.

1. **History**. Only a small number of the reputation systems use personal history, while the majority utilize global history. As the name implies, personal history is formed from the personal experiences of a single entity, and is the only type of history that can be fully relied upon. Lai et al. [49] argue that personal history does not scale well, as the chance of interacting repeatedly with the same entity is fairly small. As a result, personal history is less efficient, as other entities are not learning from your experiences. Jurca and Faltings [43] argue that personal history can be used as a form of competitive advantage in certain circumstances. They suggest that a payment scheme can be used to incentivize truthful sharing of information with others.

   RateWeb [52] proposes model where history can be fetched from a "rating clique". However, the members of these groups still act as individuals.

   Global history is available to either everyone, or the members of a selected group. Lai et al. [49] notes that although global history scales well, it is vulnerable to some types of malicious attacks. Over time, a global history should give a consistent, long-term view of an entity that approximates a relationship [66].
2. **Context**. The majority of reputation systems only employ information from a single context. The systems that allow information from multiple contexts to be utilized by members differ substantially.

   PeerTrust [94] incorporates two additional forms of contextual information; transactional attributes and a community-based context. The transactional attributes include the value of the trades being participated in, such that users can establish which trades are most relevant to their current situation. The community-based context is used to measure the level of participation within the community, for example, whether an entity often provides feedback.

   Regret [73] expands on PeerTrust and stores reputation information in the form of a vector. Individual reputation values are associated with each contextual attribute, such as the chance to overcharge, deliver late or provide a low quality item. Sabater and Sierra have also extended the Regret system to include a social context for reputation information, where trust is extracted from groups and communities (the professional and organizational rings from our model) to which an entity belongs [71].
3. **Collection**. The majority of systems use some combination of direct experience and individual indirect. Tong and Zhang [85] argue data is more reliable if collected directly rather than through a third party. The authors state that inaccuracies and lying reputation sources are reason enough to promote the direct observation collection technique. Indirect approaches involve information being obtained from other entities based on transactions that the querying entity was not privy to.

   EigenTrust [44] explains that utilizing both an individual's personal experience as well as other's indirect experience allows for making better decisions. Third party entities can be discovered and queried in a variety of ways. However, information received from others that have been discovered through either single or multiple-hop transitive trust chains should be more reliable than that discovered by querying a random entity in the network [98].

   RateWeb [52] proposes a collection model that involves a set of trusted entities being contained within each entity. When making a decision on whether or not to interact with another entity in the environment, the trusted entities are consulted for their historic actions with the target entity. RateWeb also suggests another method of indirect collection using groups and communities.

   GRAft [33,34] derives information from non-explicit reputation sources and uses it during the evaluation of policies, or to augment existing information about an entity. Case studies examine the use of derived information in policies for access control, and sharing in the social cloud. For example, derived information used by GRAft includes the Hirsch Index [36], "degree of co-authorship", "degree of friendship" and social interactivity.
4. **Representation**. Commercial systems mostly favor a representation of the reputation that utilizes both a numerical value and textual content. Academic systems however tend to exhibit a range of representations, although textual content is not as prevalent as in the commercial systems.
5. **Aggregation**. Most commercial, and many early academic systems use a simple counting-based aggregation, either by summing all of the ratings together, or providing an average. None of the systems surveyed utilized a discrete model of aggregation, probably because of the non-optimal computation aspects of aggregation with this model.

**Table 1**
Summary of academic reputation systems (see Refs. [99,73,70,3,41,8,16,44,31,76,94,40,19,79,78,61,101,28,13,100,52,85,84,5,60,33,34,95]).

| Reputation System | 01. History P=Personal G=Global | 02. Context S=Single M=Multiple A=Attribute | 03. Collection DE=Direct Experience DO=Direct Observation II=Indirect Individual IG=Indirect Group DN=Derived | 04. Representation B=Binary, D=Discrete C=Continuous S=String, V=Vector | 05. Aggregation C=Counting, D=Discrete P=Probabilistic Z=Fuzzy, F=Flow | 06. Entities I=Individual G=Group | 07. Presence O=Online P=Partial X=Offline | 08. Governance C=Centralized D=Distributed | 09. Fabric S=Structured U=Unstructured | 10. Interoperability O=Open C=Closed | 11. Control I=Incentives/Disincentives R=Rules | 12. Evaluation H=Holistic A=Atomistic | 13. Data Filtering N=None R=Recent Subset S=Selected Subset | 14. Data Aging N=None, C=Decay D=Death of Selected T=Death of Old |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Histos [99] | P | S | DE&II | C | C | I | O | ? | ? | O | ? | H | R | N |
| Sporas [99] | G | S | II | C | C | I | O | ? | ? | O | I | H | N | T |
| Regret [73, 70] | G | M‖A | DE&II&IG | D&V | C | I | O | ? | U | O | ? | H | N | C |
| P-Grid [3] | G | S | DE&II | B | C | I | O | D | S | O | I | H&A | N | N |
| Beta [41] | ? | S | ? | ? | P | ? | O | C | U | O | ? | ? | ? | ? |
| Confidant [8] | G | S | DE&DO&II | ? | ? | I | O | D | S | O | I | H | N | T |
| XRep [16] | P | S | II | B&D‖C | C | I | O | D | U | O | I | H | N | N |
| EigenTrust [44] | G | S | DE&II | C | F | I | O | D | S | O | I | H | S | N |
| Gupta et al. [31] | G | S‖A | DE&II | D&C | C | I | O | C | U | O | I | H | N | C |
| TrustMe [76] | G | S | II | ? | C | I | O | D | U | O | ? | H | N | N |
| PeerTrust [94] | G | M‖A | DE&II | C | C | I | O | D | S | O | I | H | R | N |
| Ismail et al. [40] | G | S | DE | D | na | I | P | C | U | O | na | H | S | N |
| Pride [19] | P | S | DE | ? | ? | I | P | D | U | O | I | H | N | N |
| TrustGuard [79] | G | S | II | C | C | I | O | D | S | O | I | H | N | T |
| FuzzyTrust [78] | G | S | DE&II | ? | Z | I | O | D | S | O | ? | ? | N | C |
| Travos [61] | ? | S | ? | ? | P | ? | O | D | U | O | ? | ? | ? | ? |
| PowerTrust [101] | G | S | DE | B&C&V | F | I | O | D | S | O | I | H | S | N |
| Gal-Oz et al. [28] | G | na | DE&II | V | C | I&G | O | ? | ? | O | I | H | ? | C |
| Coner et al. [13] | G | S‖A | DE | C&S | C | I | O | D | U | O | I | H&A | N | N |
| H-Trust [100] | P&G | S | II | B‖C | C | I&G | O | D | S | O | ? | H | S | C |
| RateWeb [52] | G | S | DE&II | D&C&V | C | I | O | ? | U | O | I | H | R | N |
| Tong and Zhang [85] | G | na | DE&DO | C | C | I&G | O | ? | U | O | I | na | N | N |
| $R^2$Trust [84] | P&G | S | DE&II | C | P | I | O | D | U | O | I | ? | ? | C |
| ReDS [5] | G | S | DE | C | C | I | O | D | S | O | ? | ? | N | N |
| Tulungan [60] | G | S | II | ? | ? | I | O | C | ? | O | I | ? | ? | ? |
| GRAft [33, 34] | G | M‖A | DE&DN | D&C&S | na | I | P | D | S | O | I | H&A | N | N |
| PerContRep [95] | G | S | DE | ? | C | I | O | C | ? | O | ? | ? | N | C |

**Table 2**
Summary of commercial reputation systems (see Refs. [4,6,14,21,25,26,58,32,65,77,80,87–89,96]).

| Reputation System | 01. History P=Personal G=Global | 02. Context S=Single M=Multiple A=Attribute | 03. Collection DE=Direct Experience DO=Direct Observation II=Indirect Individual IG=Indirect Group DN=Derived | 04. Representation B=Binary, D=Discrete C=Continuous S=String, V=Vector | 05. Aggregation C=Counting, D=Discrete P=Probabilistic Z=Fuzzy, F=Flow | 06. Entities I=Individual G=Group | 07. Presence O=Online P=Partial X=Offline | 08. Governance C=Centralized D=Distributed | 09. Fabric S=Structured U=Unstructured | 10. Interoperability O=Open C=Closed | 11. Control I=Incentives/Disincentives R=Rules | 12. Evaluation H=Holistic A=Atomistic | 13. Data Filtering N=None R=Recent Subset S=Selected Subset | 14. Data Aging N=None, C=Decay D=Death of Selected T=Death of Old |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Advogato [4] | G | S | DE | D | C | I | O | C | ? | C | I | H | N | N |
| Amazon [6] | G | S | DE | B&D&S | C | I | O | C | ? | C | I | H | S | N |
| Couchsurfing [14] | G | S | DE | D&S | C | I | O | C | ? | C | I | H&A | S | N |
| Digg [21] | G | S | DE&II | D | C | I | O | C | ? | O | I | H | N | N |
| eBay [25] | G | S‖A | DE | D&S | C | I | O | C | ? | C | I | H&A | S | T |
| ePinions [26] | G | S | DE | D&S | C | I | O | C | ? | C | I | H&A | S | N |
| MTurk [58] | G | S‖A | DE | D | C | I | O | C | ? | C | I | H&A | N | N |
| PageRank (Google) [32] | G | S | DE | D&C | F | I | O | C | ? | C | na | H | N | N |
| Reddit [65] | G | S | DE | D | C | I | O | C | ? | C | I | H | N | N |
| SlashDot (Karma) [77] | G | S | DE | D&C | C | I | O | C | ? | C | I | H | N | N |
| Stackoverflow [80] | G | S | DE&II | D | C | I | O | C | ? | C | I | H&A | N | N |
| TrustedSource [87] | G | S | DE | D | C | I | O | C | ? | C | R | H&A | N | C |
| Trustribe [88] | G | S‖A | DE&II | D&S | C | I | O | C | ? | O | I | H | N | N |
| Turkopticon [89] | G | S‖A | DE | C&S | C | I | O | C | ? | C | I | H&A | N | N |
| Yelp [96] | G | S | DE | D&S | C | I | O | C | ? | C | I | H&A | S | C |

Beta [41] and Travos [61] both implement a probabilistic approach using the Beta probability density function, as this is considered suitable for processing binary ratings [97].

EigenTrust [44] utilizes a flow approach to calculating global reputation values. In particular, global reputation values are calculated using the "left principal eigenvector of a matrix of normalized local trust values". The local, or personal, trust values in EigenTrust are sums of the positive and negative ratings. PowerTrust [101] employs a similar approach to EigenTrust, but uses a Bayesian method to calculate the personal trust values.

A fuzzy approach to aggregation is utilized by FuzzyTrust [78] when aggregating personal trust ratings.

GRAft [33,34] does not employ any aggregation; it is up to the trustor to interpret the reputation information stored in the network.

6. **Entities**. The concept of group reputation is introduced by Mui et al. [56]. Barring three exceptions, all reputation systems that we have classified in our taxonomy focus on individuals. These individuals could be either people or specific resources.

The first exception is the work presented by Gal-Oz et al. [28], where communities are broken down into smaller sub-communities the authors call "knots". Knots are formed from community members who have strong trust relationships amongst themselves. The reputation information within a knot is therefore more valuable and is given a higher weighting.

The second exception is the work presented by Tong and Zhang [85]. In their paper, they propose using direct observation of the size of the group to determine its reputation. If individual entities are seen to be joining a group, then clearly that group has a positive reputation, and vice-versa. Although not explicitly stated, they are in fact looking at the size of the group over a period of time. A simplified view of group reputation is basically the change in the number of members over time.

The last exception is discussed in Zhao and Li [100], where nodes are able to calculate the reputation of other entities, either individuals or groups, using their own private history and choice of algorithm.

Finally, although Regret does not support group entities directly, Sabater and Sierra introduce the idea of a "neighborhood reputation" that is based on the reputation and relationships of neighboring entities to the target entity. A given entity therefore inherits a reputation by default, allowing even entities that are less well known to have reputation.

7. **Presence**. Of the systems examined, none is fully offline, and only Ismail et al. [40] and Pride [19] support a partial presence. The former talks about distributing reputation information to third-parties via certificates. An authority is utilized to create the certificates, but not needed to distribute and interpret the information contained within them.

   The latter introduces the Pride reputation system which has been constructed for decentralized peer-to-peer networks. The system enables self-certification of entities with digital certificates and employs an elicitation storage protocol to distribute reputation information.
8. **Governance**. Most commercial reputation systems exhibit centralized governance, including Amazon, eBay and ePinions. The terms *centralized* and *distributed* are most often used in conjunction with the description of reputation system architecture such as in Wang and Vassileva [91], Jøsang et al. [42], Gupta et al. [31], Dutta et al. [23] and Wang and Li [90]. However, it is often difficult to establish with any degree of certainty how a given reputation system is actually implemented, particularly commercial systems that rarely provide operational details. For example, in Wang and Vassileva [91] eBay is noted as being centralized, when in reality it may well be distributed in order to cope with the traffic load. However, we can say that the system has centralized governance.
9. **Fabric**. There is a good mix of systems showing both structured and unstructured characteristics. PowerTrust [101] employs a structured approach to reputation collection and aggregation. The system utilizes a trust overlay network to model transactions and nominates trustworthy entities as power nodes, responsible for aggregating global reputation scores.
10. **Interoperability**. Although reputation information within academic systems is often freely accessible, none of the systems that we surveyed had any explicit support for importing or exporting reputation information.

    For a short period of time, Amazon allowed its members to import their feedback scores from eBay, effectively removing the need to establish a new reputation. However, once legal action was taken, Amazon was forced to remove this functionality [66].
11. **Control**. The control category is often overlooked due to an underlying assumption that trustworthy users are rewarded. The practice of disincentivizing entities in a reputation system is also not trivial. The following examples demonstrate a disincentive technique to promote good behavior in the environment, however the environment itself is typically restricted. Confidant [8], for example, utilizes the disincentive principle, by placing consequences on badly-behaved routers. Once entities are discovered that appear to be acting maliciously, Confidant works to restrict the use of that router in future transmissions.

    P-Grid [2], is another system that punishes rather than rewards certain behavior. Entities within the system are assumed to be co-operative, meaning that only malicious behavior has an effect on one's reputation score. Both of these examples occur in a system where entities can easily be neglected and avoided. Other environments that use reputation systems may not be able to enforce such penalties as easily. For example, in a Grid setting, the process of excluding an entity from joining a virtual organization can be extremely costly if they provide a sufficiently limited resource.
12. **Evaluation**. All systems surveyed for this taxonomy implement a holistic evaluation of the trustee. A small number of the systems also support an atomistic evaluation method, allowing the user to drill-down on particular aspects of the available information.
13. **Data Filtering**. Filtering is employed by a few systems. RateWeb [52] uses an approach where the trustors in the system apply limitations on data to determine what is too old to be considered useful. RateWeb includes a method called "reputation fading". Each rating is time-stamped, allowing newer feedback to be given a higher weighting when computing reputation scores. This is considered data filtering and not data aging because the data is not discarded, but rather filtered by the trustor.
14. **Data Aging**. A number of systems implement Data Aging. The Regret [71] system provides a time-dependent method to calculate an individual reputation. As information gets older, its weight in the calculation diminishes. The authors cite Karlins and Abelson [45] as support for the feature. Zacharia et al. [99] implements a method to age and remove information through a "dumping function". The authors state that larger amounts of feedback increase the accuracy of the reputation system. Due to entities being able to alter their behavior at will, the authors assert that it is beneficial to disregard old ratings to move the behavior predicted by the reputation system closer to an entity's current performance.

## 6. Related taxonomies

In Mui et al. [56], the authors present a reputation typology. This typology includes only a small number of dimensions as it tries to combine reputational literature from a number of different disciplines.

A set of classification dimensions for trust and reputation models is introduced in Sabater and Sierra [72]. These are subsequently used to classify a number of well-known trust and reputation systems. This work does not consider a number of the dimensions that are present in our taxonomy.

A taxonomy for P2P reputation systems is introduced in Marti and Garcia-Molina [53]. The goal of their paper is to organize existing ideas and work, so that design and implementation can be better achieved. They have 11 dimensions in three areas of interest: information gathering, scoring and ranking, and response.

A framework for the comparison of reputation-based trust systems for P2P applications is presented in Koutrouli and Tsalgatidou [48]. The authors investigate 14 dimensions, spread across three key areas of interest: information gathering, feedback aggregation and output. The focus of this paper is on P2P e-commerce, file sharing and co-operative applications.

In Wang and Vassileva [91], the authors introduce a classification of trust and reputation systems based on system structure. Their particular focus is on using trust and reputation information for web-service selection. The three classification criteria discussed in their paper are each directly related to the underlying architecture of the reputation system. Although aspects of system structure are identified by our work, we also consider other details in the classification.

A survey of trust and reputation systems is presented in Jøsang et al. [42]. The authors focus on and thoroughly investigate reputation calculation, and how it is implemented in currently deployed systems.

In Hoffman et al. [37], the authors present a survey of attack and defense techniques for reputation systems. An analytical framework for breaking down and comparing reputation systems is introduced in order to identify common issues. This framework considers aspects such as dissemination and calculation of reputation. They also discuss existing reputation systems in the context of security weaknesses and the defenses that are employed by these systems.

A taxonomy of attacks for P2P reputation systems is presented in Koutrouli and Tsalgatidou [47]. Their taxonomy breaks down reputation attacks into three primary categories: Unfair recommendations, Inconsistent behavior and Identity management attacks. The authors then present a series of defense mechanisms, and conclude with a roadmap for system designers.

Yao et al. [97] address common vulnerability issues in reputation systems. As part of their work they present a "decomposition" of reputation systems that examines dissemination and calculation in a number of systems.

## 7. Supplementary characteristics and ideas for future research

In addition to the dimensions of the taxonomy, we identified a number of adjunct characteristics that may be topical in reputation systems research.

- The integration of machine and human entities within reputation systems has not been discussed in this taxonomy, however it is an area that requires wider research. In order to determine whether or not human and machine users can and should be incorporated into a single reputation system, the differences between the two need to be defined. The complexities associated with such a merger, the cohesion of their characteristics, differences in performance measurement, and malicious attacks made possible should also be considered.
- Implicit support for the import and export of reputation information is another area for further research. The ability to import and export reputation information becomes more complex as the contexts vary. For the base-case of exchanging information between systems with similar contexts, we only require a set of standards that describe how reputation information should be encoded and exchanged. For more complex cases, where systems have differing contexts, this would require a set of standards that enumerate the contexts, and a way to generalize reputation values as they move between these contexts. Initial work in this space can be found in [29], where the authors introduce a Cross-Community Reputation (CCR) model that allows for the transfer of reputation information between different communities.
- The integration of identity and reputation is not widely considered, and requires further thought. In particular, storing reputation information along with identity information would help in the transfer of reputation between different contexts, and would aid in the bootstrapping of existing users on a new system. Further, the ability to centralize both identity and reputation information would help to break down reputation silos and make reputation information more useful in a wider sense. Initial work in this direction, utilizing OpenID, can be found in GRAft [33] and Tormo et al. [86].
- Similarly, the ability to utilize reputation as a service is only just in its infancy. As with any other service, being able to query and update reputation as a service would be useful in many environments. Hillebrand and Coetzee [35] discuss using reputation as a service in cloud environments, while in [33,34] the authors provide case-studies that examine the use of reputation in access control and sharing of resources in the cloud.

## 8. Conclusion

In this paper we have presented a detailed categorization for reputation systems. We have surveyed a large number of reputation systems and created a definitive taxonomy to describe their architecture and organization. In addition to the taxonomy we have proposed a new reference model for context and a general interaction model for reputation systems. The taxonomy was exercised on a number of reputation systems, and the resulting analysis shows that our taxonomy is a useful tool for examining and comparing reputation systems. The application of our taxonomy has identified several areas of reputation systems that are currently under-represented in research:

- Contextual information is still largely under-utilized within reputation systems. Reputation information is context dependent, however few reputation systems support more than a single context. Wider investigation is required into the maintenance and utilization of information from multiple contexts. In particular, the aggregation of contextual information into a single value for consumption, or maintaining distinct values. The importance and procedures behind the exchange of reputation information between distinct reputation systems is a current weak area of the current research.
- Derived information sources also require wider investigation. In particular, the identification of derivable reputation sources, the ability to aggregate and utilize the derived information within a reputation system, and the policies to integrate and embed distinct sources and destinations. The value of including derived information from abstract sources that were not explicitly designed to generate information for decision making is a rich area for novel research.
- Individual entities are pervasive in current reputation systems. There is little material on group entities. Group entities have an important role to play in future reputation systems. In a virtual organization, individual and group entities may join together temporarily to solve a common problem or work on a task. Reputation can play a key role in such environments.
- Although partial presence is exhibited by three of the systems we examined, none of the systems had the ability to distribute reputation information fully-offline. The ability to operate fully-offline would allow for robust decentralized reputation systems.

As more and more people come to rely on online services and communities, reputation systems will play an increasingly important role in facilitating their interactions. It is already apparent that online services can play a profound role in a person's life, both personal and professional. A reputation forged online is increasingly being used to screen both current, and possible future employees. A single false move is potentially remembered forever, causing a long-lasting reputational "stain" on an otherwise normal person's life.

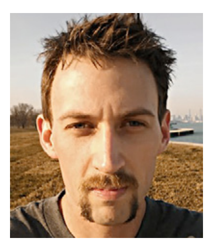
## References

[1] A. Abdul-Rahman, S. Hailes, Supporting trust in virtual communities, in: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, IEEE, 2000, p. 9.
[2] K. Aberer, A. Datta, Z. Despotovic, M. Hauswirth, M. Punceva, R. Schmidt, P-Grid: A Self-organizing Structured P2P System, Jul. 28 2003.
[3] K. Aberer, Z. Despotovic, Managing trust in a peer-2-peer information system, in: CIKM'01: Proceedings of the Tenth International Conference on Information and Knowledge Management, ACM, New York, NY, USA, 2001, pp. 310–317.
[4] Advogato, http://www.advogato.org/, last accessed 2014-04-07.
[5] R. Akavipat, M. Al-Ameen, A. Kapadiau, Z. Rahman, R. Schlegel, M. Wright, ReDS: A Framework for Reputation-Enhanced DHTs.
[6] Amazon, http://www.amazon.com/, last accessed 2014-04-07.
[7] E. Bagheri, A.A. Ghorbani, Behavior analysis through reputation propagation in a multi-context environment, in: PST'06: Proceedings of the 2006 International Conference on Privacy, Security and Trust, ACM, New York, NY, USA, 2006, pp. 1–7.
[8] S. Buchegger, J.-Y.L. Boudec, Performance analysis of the CONFIDANT protocol, in: Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking & Computing, ACM, 2002, pp. 226–236.
[9] N. Capon, Credit scoring systems: A critical analysis, J. Marketing (1982) 82–91.
[10] S. Casare, J. Sichman, Towards a functional ontology of reputation, in: AAMAS '05: Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, ACM, New York, NY, USA, 2005, pp. 505–511.
[11] K. Chard, K. Bubendorfer, S. Caton, O. Rana, Social cloud computing: A vision for socially motivated resource sharing, IEEE Trans. Serv. Comput. 5 (4) (2012) 551–563.
[12] K. Chard, S. Caton, O. Rana, K. Bubendorfer, Social cloud: Cloud computing in social networks, in: Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, IEEE, 2010, pp. 99–106.
[13] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, K. Nahrstedt, A trust management framework for service-oriented environments, in: WWW'09: Proceedings of the 18th International Conference on World Wide Web, ACM, New York, NY, USA, 2009, pp. 891–900.
[14] Couchsurfing, http://www.couchsurfing.org/, last accessed 2014-04-07.
[15] N. Curtis, R. Safavi-Naini, W. Susilo, $X^2$Rep: Enhanced trust semantics for the XRep Protocol, Lecture Notes in Comput. Sci. 3089 (2004) 205–219.
[16] E. Damiani, D.C. di Vimercati, S. Paraboschi, P. Samarati, F. Violante, A reputation-based approach for choosing reliable resources in peer-to-peer networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS'02, ACM, New York, NY, USA, 2002, pp. 207–216.
[17] C. Dellarocas, The digitization of word of mouth: Promise and challenges of online feedback mechanisms, Manage. Sci. 49 (2003) 1407–1424.
[18] Z. Despotovic, K. Aberer, Possibilities for Managing Trust in P2P Networks, Tech. Rep., Swiss Federal Institute of Technology, Zurich, Switzerland, 2004.
[19] P. Dewan, P. Dasgupta, Pride: Peer-to-Peer reputation infrastructure for decentralized environments, in: WWW Alt.'04: Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers & Posters, ACM, New York, NY, USA, 2004, pp. 480–481.
[20] A.K. Dey, G.D. Abowd, Towards a better understanding of context and context-awareness, in: HUC'99: Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing, Springer-Verlag, 1999, pp. 304–307.
[21] Digg, http://digg.com/, last accessed 2014-04-07.
[22] A. Doan, R. Ramakrishnan, A.Y. Halevy, Crowdsourcing systems on the world-wide web, Commun. ACM 54 (2011) 86–96.
[23] D. Dutta, A. Goel, R. Govindan, H. Zhang, The design of a distributed rating scheme for Peer-to-Peer systems, in: The 1st Workshop on Economics of Peer-to-Peer Systems, 2003.
[24] Dropbox, http://www.dropbox.com/, last accessed 2014-04-07.
[25] eBay, http://www.ebay.com/, last accessed 2014-04-07.
[26] ePinions, http://www.epinions.com/, last accessed 2014-04-07.
[27] Facebook, http://www.facebook.com/, last accessed 2014-04-07.
[28] N. Gal-Oz, E. Gudes, D. Hendler, A Robust and knot-aware trust-based reputation model, in: Y. Karabulut, J. Mitchell, P. Herrmann, C. Jensen (Eds.), Trust Management II, in: IFIP—The International Federation for Information Processing, vol. 263, Springer US, 2008, pp. 167–182.
[29] T. Grinshpoun, N. Gal-Oz, A. Meisels, E. Gudes, CCR: A model for sharing reputation knowledge across virtual communities, in: Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology - Volume 01, WI-IAT '09, IEEE Computer Society, Washington, DC, USA, 2009, pp. 34–41.
[30] E. Gudes, N. Gal-Oz, A. Grubshtein, Methods for computing trust and reputation while preserving privacy, in: Data and Applications Security XXIII, Springer, 2009, pp. 291–298.
[31] M. Gupta, P. Judge, M. Ammar, A reputation system for peer-to-peer networks, in: NOSSDAV '03: Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video, ACM, New York, NY, USA, 2003, pp. 144–152.
[32] Google, http://www.google.com/, last accessed 2014-04-07.
[33] F. Hendrikx, K. Bubendorfer, Malleable access rights to establish and enable scientific collaboration, in: eScience (eScience), 2013 IEEE 9th International Conference on, IEEE, Beijing, China, 2013, pp. 334–341.
[34] F. Hendrikx, K. Bubendorfer, Policy derived access rights in the social cloud, in: eScience (eScience), 2013 IEEE 9th International Conference on, IEEE, Beijing, China, 2013, pp. 365–368.
[35] C. Hillebrand, M. Coetzee, Towards Reputation-as-a-Service, in: Information Security for South Africa, 2013, pp. 1–8.
[36] J.E. Hirsch, An index to quantify an individual's scientific research output, Proc. Natl. Acad. Sci. USA 102 (46) (2005) 16569.
[37] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. 42 (1) (2009) 1–31.
[38] D. Houser, J. Wooders, Reputation in auctions: Theory, and evidence from eBay, J. Econom. Manag. Strategy 15 (2) (2006) 353–369.
[39] J. Howe, The rise of crowdsourcing, Wired Magazine 14 (14) (2006) 1–5.
[40] R. Ismail, C. Boyd, A. Jøsang, S. Russell, An efficient off-line reputation scheme using articulated certificates, in: WOSIS-2004: Proceedings of the Second International Workshop on Security in Information Systems, 2004, pp. 53–62.
[41] A. Jøsang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, 2002, pp. 41–55.
[42] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.
[43] R. Jurca, B. Faltings, An incentive compatible reputation mechanism, IEEE Int. Conf. E-Commerce Technol. 0 (2003) 285.
[44] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The EigenTrust Algorithm for reputation management in P2P networks, in: Proceedings of the 12th International World Wide Web Conference, ACM, New York, NY, USA, 2003, pp. 640–651.
[45] M. Karlins, H. Abelson, Persuasion, How Opinion and Attitudes are Changed, 1970.
[46] M. Kinateder, K. Rothermel, Architecture and algorithms for a distributed reputation system, in: Proceedings of the First International Conference on Trust Management, Springer-Verlag, 2003, pp. 1–16.
[47] E. Koutrouli, A. Tsalgatidou, Taxonomy of attacks and defense mechanisms in P2P reputation systems—lessons for reputation system designers, Comput. Sci. Rev. 6 (2) (2012) 47–70.
[48] E. Koutrouli, A. Tsalgatidou, Reputation-based trust systems for P2P applications: design issues and comparison framework, Trust Privacy Digital Business (2006) 152–161.
[49] K. Lai, M. Feldman, I. Stoica, J. Chuang, Incentives for Cooperation in Peer-to-Peer Networks, 2003.
[50] LinkedIn, http://www.linkedin.com/, last accessed 2014-04-07.
[51] L. Liu, M. Munro, Systematic analysis of centralized online reputation systems, Decis. Support Syst. 52 (2) (2012) 438–449.
[52] Z. Malik, A. Bouguettaya, RATEWeb: Reputation assessment for trust establishment among Web services, VLDB J. 18 (4) (2009) 885–911.
[53] S. Marti, H. Garcia-Molina, Taxonomy of trust: Categorizing P2P reputation systems, Computer Networks 50 (4) (2006) 472–484.
[54] M.I. Melnik, J. Alm, Does a Seller's eCommerce reputation matter? Evidence from eBay Auctions, J. Industrial Economics 50 (3) (2002) 337–349.
[55] L.J. Mester, What's the point of credit scoring?, Business Rev. 3 (1997) 3–16.
[56] L. Mui, M. Mohtashemi, A. Halberstadt, Notions of reputation in multi-agent systems: A Review, in: Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems, ACM, New York, NY, USA, 2002, pp. 280–287.
[57] L. Mui, M. Mohtashemi, A. Halberstadt, A Computational model of trust and reputation, in: System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, IEEE, 2002, pp. 2431–2439.
[58] MTurk, http://www.mturk.com/, last accessed 2014-04-07.
[59] R. Nickerson, J. Muntermann, U. Varshney, H. Isaac, Taxonomy development in information systems: Developing a taxonomy of mobile applications, in: Proceedings of the European Conference on Information Systems, 2009.
[60] A. Pantola, S. Pancho-Festin, F. Salvador, TULUNGAN: A self-promoting-resistant reputation system for collaborative web filtering systems, in: The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013), The Society of Digital Information and Wireless Communication, 2013, pp. 281–292.
[61] J. Patel, W.L. Teacy, N.R. Jennings, M. Luck, A probabilistic trust model for handling inaccurate reputation sources, in: Trust Management, Springer, 2005, pp. 193–209.
[62] E. Pavlov, J.S. Rosenschein, Z. Topol, Supporting privacy in decentralized additive reputation systems, Trust Manag. (2004) 108–119.
[63] N. Poor, Mechanisms of an online public sphere: The website slashdot, J. Comput. Mediated Commun. 10 (2) (2005).
[64] J.M. Pujol, R. Sangüesa, J. Delgado, Extracting reputation in multi agent systems by means of social network topology, in: Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, AAMAS '02, ACM, New York, NY, USA, 2002, pp. 467–474.
[65] Reddit, http://www.reddit.com/, last accessed 2014-04-07.
[66] P. Resnick, K. Kuwabara, R. Zeckhauser, E. Friedman, Reputation systems, Commun. ACM 43 (2000) 45–48.
[67] P. Resnick, R. Zeckhauser, Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system, Adv. Microeconomics: A Research Annual 11 (2002) 127–157.
[68] P. Resnick, R. Zeckhauser, J. Swanson, K. Lockwood, The value of reputation on eBay: A controlled experiment, Experimental Economics 9 (2003) 79–101.
[69] S. Ruohomaa, L. Kutvonen, E. Koutrouli, Reputation management survey, in: The Second International Conference on Availability, Reliability and Security, ARES 2007, 2007, pp. 103–111.

[70] J. Sabater, C. Sierra, REGRET: Reputation in gregarious societies, in: Proceedings of the Fifth International Conference on Autonomous Agents, AGENTS'01, ACM, New York, NY, USA, 2001, pp. 194–195.
[71] J. Sabater, C. Sierra, REGRET: Reputation in gregarious societies, in: AGENTS '01: Proceedings of the Fifth International Conference on Autonomous Agents, ACM, New York, NY, USA, 2001, pp. 194–195.
[72] J. Sabater, C. Sierra, Review on computational trust and reputation models, Artificial Intelligence Rev. 24 (2005) 33–60.
[73] J. Sabater, C. Sierra, Social ReGreT, a reputation model based on social relations, SIGecom Exch. 3 (1) (2002) 44–56.
[74] A. Schlosser, M. Voss, L. Brückner, On the simulation of global reputation systems, J. Artif. Soc. Social Simul. 9 (2005) 1.
[75] C. Selvaraj, S. Anand, A survey on security issues of reputation management systems for Peer-to-Peer networks, Computer Sci. Rev. 6 (4) (2012) 145–160.
[76] A. Singh, L. Liu, TrustMe: Anonymous management of trust relationships in decentralized P2P systems, in: Proceedings of the Third International Conference on Peer-to-Peer Computing, P2P 2003, 2003, pp. 142–149.
[77] Slashdot, http://slashdot.org/, last accessed 2014-04-07.
[78] S. Song, K. Hwang, R. Zhou, Y.-K. Kwok, Trusted P2P transactions with fuzzy reputation aggregation, Internet Computing, IEEE 9 (6) (2005) 24–34.
[79] M. Srivatsa, L. Xiong, L. Lui, TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks, in: Proceedings of the 14th International Conference on World Wide Web, WWW'05, ACM, New York, NY, USA, 2005, pp. 422–431.
[80] Stackoverflow, http://stackoverflow.com/, last accessed 2014-04-07.
[81] S. Steinbrecher, Design options for privacy-respecting reputation systems within centralised internet communities, in: S. Fischer-Hübner, K. Rannenberg, L. Yngström, S. Lindskog (Eds.), Security and Privacy in Dynamic Environments, in: IFIP International Federation for Information Processing, vol. 201, Springer Boston, 2006, pp. 123–134.
[82] D.W. Sue, Multidimensional facets of cultural competence, The Counseling Psychologist 29 (6) (2001) 790–821.
[83] M. Tavakolifard, S.J. Knapskog, P. Herrmann, Trust transferability among similar contexts, in: Q2SWinet'08: Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, ACM, New York, NY, USA, 2008, pp. 91–97.
[84] C. Tian, B. Yang, $R^2$trust, a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks, Future Gener. Comput. Syst. 27 (8) (2011) 1135–1141.
[85] X. Tong, W. Zhang, Group trust and group reputation, in: ICNC'09: Proceedings of the 2009 Fifth International Conference on Natural Computation, IEEE Computer Society, Washington, DC, USA, 2009, pp. 561–565.
[86] G.D. Tormo, F.G. Mármol, G.M. Pérez, Towards the integration of reputation management in OpenID, Comput. Standards Interfaces 36 (3) (2014) 438–453.
[87] TrustedSource, http://www.trustedsource.org/, last accessed 2014-04-07.
[88] Trustribe, http://www.trustribe.com/, last accessed 2014-04-07.
[89] Turkopticon, http://turkopticon.differenceengines.com/, last accessed 2014-04-07.
[90] C. Wang, B. Li, Peer-to-Peer Overlay Networks: A Survey, Tech. Rep., The Hong Kong University of Science and Technology, 2003.
[91] Y. Wang, J. Vassileva, Toward trust and reputation based web service selection: A Survey, Int. Trans. Syst. Sci. Appl. 3 (2) (2007) 118–132.
[92] Wikipedia, http://www.wikipedia.org/, last accessed 2014-04-07.
[93] K. Wongrujira, A. Seneviratne, Monetary incentive with reputation for virtual market-place based P2P, in: CoNEXT'05: Proceedings of the 2005 ACM Conference on Emerging Network Experiment and Technology, ACM, New York, NY, USA, 2005, pp. 135–145.
[94] L. Xiong, L. Liu, PeerTrust: Supporting reputation-based trust for Peer-to-Peer electronic communities, IEEE Trans. Knowledge Data Eng. 16 (7) (2004) 843–857.
[95] Z. Yan, Y. Chen, Y. Shen, PerContRep: a practical reputation system for pervasive content services, J. Supercomput. (2014) 1–24.
[96] Yelp, http://www.yelp.com/, last accessed 2014-04-07.
[97] Y. Yuan, S. Ruohomaa, F. Xu, Addressing common vulnerabilities of reputation systems for electronic commerce, J. Theoret. Appl. Electron. Commerce Res. 7 (1) (2012) 1–20.
[98] B. Yu, M.P. Singh, A social mechanism of reputation management in electronic communities, in: Proceedings of Fourth International Workshop on Cooperative Information Agents, 2000, pp. 154–165.
[99] G. Zacharia, A. Moukas, P. Maes, Collaborative reputation mechanisms for electronic marketplaces, Decis. Support Syst. 29 (4) (2000) 371–388.
[100] H. Zhao, X. Li, H-Trust: A group trust management system for Peer-to-Peer desktop grid, J. Comput. Sci. Tech. 24 (2009) 833–843.
[101] R. Zhou, K. Hwang, PowerTrust: A robust and scalable reputation system for trusted Peer-to-Peer computing, IEEE Trans. Parallel Distrib. Syst. 18 (2007) 460–473.

**Ferry Hendrikx** is a Ph.D. student at the School of Engineering and Computer Science, Victoria University of Wellington. His research interests include distributed, peer-to-peer and reputation systems. Apart from his studies, he is a self-employed ICT Consultant with 15 years of experience. He works mainly for government agencies and private companies in Wellington, New Zealand.

**Kris Bubendorfer** is a Senior Lecturer in Network Engineering at Victoria University of Wellington. He received his Ph.D. in Computer Science, on a mobile agent middleware, from the Victoria University of Wellington in 2002. His current research interests include distributed computing, social computing, digital provenance and reputation. He teaches courses in networking, operating systems, security and distributed systems.



**Ryan Chard** is a Ph.D. student at the School of Engineering and Computer Science, Victoria University of Wellington. His research interests include distributed systems, social computing, cloud computing and reputation. He actively teaches undergraduate computer science courses.