IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 6, 2020, accepted June 14, 2020, date of publication July 16, 2020, date of current version August 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009445

A Survey on Trust Prediction in Online Social Networks

SEYED MOHSSEN GHAFARI[1], AMIN BEHESHTI[1], ADITYA JOSHI[2], CECILE PARIS[2], ADNAN MAHMOOD[1], SHAHPAR YAKHCHI[1], AND MEHMET A. ORGUN[1], (Senior Member, IEEE)

[1]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[2]CSIRO Data61, Marsfield, NSW 2122, Australia

Corresponding author: Seyed Mohssen Ghafari (seyed-mohssen.ghafari@hdr.mq.edu.au)

The work of Seyed Mohssen Ghafari was supported by the Data61, in July 2018.

ABSTRACT Level of Trust can determine which source of information is reliable and with whom we should share or from whom we should accept information. There are several applications for measuring trust in Online Social Networks (OSNs), including social spammer detection, fake news detection, retweet behaviour detection and recommender systems. Trust prediction is the process of predicting a new trust relation between two users who are not currently connected. In applications of trust, trust relations among users need to be predicted. This process faces many challenges, such as the sparsity of user-specified trust relations, the context-awareness of trust and changes in trust values over time. In this paper, we analyse the state-of-the-art in pair-wise trust prediction models in OSNs, classify them based on different factors, and propose some future directions for researchers interested in this field.

INDEX TERMS Context-aware, data sparsity problem, online social networks, pair-wise trust prediction, trust, trust relations, time-aware.

I. INTRODUCTION

In early human societies, (hunter-gatherer) people realised that to fulfil their needs, they had to interact with each other. Quickly, they found that not all interactions were beneficial for them. For instance, their experiences in trading with other people (traders) were not always satisfactory, and sometimes they were deceived by the traders. At that point, they learned to interact with trustworthy people. Trust can be defined as the 'willingness of a party to be vulnerable to actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party' [1]. 'Trust is necessary in order to face the unknown, whether that unknown is another human being, or simply the future and its contingent events'.[1] Sociologically speaking, 'a complete absence of trust would prevent [one] even getting up in the morning' [2].

There are several applications for measuring trust levels in Online Social Networks (OSNs), including social spammer detection [3], fake news detection [4], retweet behaviour detection [5], [6], recommender systems [7], [8] and influence spread problem [9], [10]. Trust prediction can be defined as the process of predicting a new trust relation between a pair of users that may not be connected in a social network. In applications of trust, trust relations among users need to be predicted. This process faces many challenges, such as the sparsity of user-specified trust relations, the context-awareness of trust and changes in trust values over time.

Although, there were some minor attempts in providing overviews on trust prediction approaches, they either mainly focus on one particular type of trust prediction approaches (Liu *et al.* [11] mainly focus on supervised trust prediction approaches) or they have been published several years ago and they may fail to overview the trust prediction approaches that were proposed in recent years [12]–[14]. In this paper, we aim to find the research gaps in the literature of trust, classify the state-of-the-art pair-wise trust prediction models based on how they address the research gaps, and finally suggest some future direction for researchers in this field.

The rest of the paper is organised as follows: Section II-A provides various definitions for the concept of trust from different aspects. Sections II and IV discuss the required

The associate editor coordinating the review of this manuscript and approving it for publication was Renato Ferrero.

[1]https://reviews.history.ac.uk/review/287a

preliminaries and challenges of trust prediction process. We present the properties of trust, mechanisms for collecting trust information and the ways to present trust in Sections II-B, II-C and III. We discuss the trust prediction process and the current state-of-the-art approaches in Sections II-E and V. Finally, we present the related studies on the impact of users' personality on trust and suggest some future directions for researchers in Sections V-E and IX, before concluding the paper in Section X.

II. PRELIMINARIES

This section briefly introduces the main concepts of this paper.

A. DEFINITION OF TRUST

With the development of human societies, trust has played an important role in people's lives, including in their relationships, families and their businesses and in social management systems. With the development of science and scientific knowledge, different branches of science that focused on human behavioural analysis and human interaction analysis started to study the concept of trust. Trust has different definitions in different scientific fields. Here, a brief overview is provided on the definition of trust in psychology, sociology, economics and, of particular relevance to the subject of this paper, computer science.

1) TRUST IN PSYCHOLOGY

Schlenker *et al.* [15] provided a definition for trust: being confident about received information from another party in an uncertain environmental state. Psychologists also define trust as 'the subjective probability by which an individual expects that another performs a given action on which its welfare depends' [14]. Psychologically speaking, an inclination towards trusting others can be considered a personality trait [13]. Moreover, 'trusting behaviour takes place when an individual confronts an ambiguous path leading to a perceived either beneficial or harmful result contingent on the action of another person' [16].

2) TRUST IN SOCIOLOGY

Although in sociology studies, the main focus is on the trust in the society or social relations, some research has also focused on trust at the individual level. At this level, the definition of trust is similar to that in psychology [16]; for example, Sztompka stated that 'trust is a bet about the future contingent actions of others' [17]. At the society or social relations level, sociologists consider trust as a properties of social groups [16] and define it as 'a set of expectations shared by all those involved in an exchange' [18]. Another sociologist defined trust as 'a means for reducing the complexity of society' [2]. A different definition of trust was provided by Seligman [19]: 'trust enters into social interaction in the interstices of systems, when for one reason or another systematically defined role expectations are no longer viable'. Hence, according to Seligman, if people play their expected roles, we can safely have our own transactions [19].

3) TRUST IN ECONOMICS

In economics, trust is defined as 'the property of a business relationship, such that reliance can be placed on the business partners and the business transactions developed with them' [20]. Economists also conceptualise trust as 'existing when one party has confidence in an exchange partner's reliability and integrity' [21]. Moreover, in online trading environments, where there is a lack of direct interaction with customer and products, 'trust can reduce transaction risks, mitigate information asymmetry and generate price premiums for reputable vendors' [16], [22], [23].

4) TRUST IN COMPUTER SCIENCE

The concept of trust is widely used in computer science. Artz and Gil [24] classified trust related research domains in computer science into four major categories: i) policy-based trust, which covers studies in topics related to network security credentials, security policies and trust languages; ii) reputation-based trust, which includes research on trust in peer-to-peer networks, and grids and trust metrics in a web of trust; iii) general models of trust, encompassing research addressing general considerations and properties of trust and software engineering; and iv) trust in information resources, which focus on trust concerns on the Web, the semantic Web and information filtering based on trust.

Trust also plays a significant role in the online activities of users of platforms such as Online Social Networks (OSNs). Tang *et al.* [25] provided a popular definition for trust in OSNs: 'Trust provides information about with whom we should share information, from whom we should accept information and what considerations to give to information from people when aggregating or filtering data'. There are many applications for trust in OSNs, including: social spammer detection [3], fake news detection [4], retweet behaviour detection [5], [6] and recommender systems [7], [8]. All these applications require predicting the trust relations among users.

B. PROPERTIES OF TRUST

The properties of trust have been listed as context-specific, dynamic, propagative, subjective, asymmetric and event sensitive [12]. We should keep in mind that trust is a concept that is not closed to the specific OSN studied, because it depends on ethical, social, cultural, historical aspects outside the network as well. This is beyond the property of Context Specific, because it only refers to topics that can be developed within the same social network (e.g. science, arts, politics, sports, etc.). However, our intention in this paper is to analyze features of trust relations that can be found within the OSNs.

1) CONTEXT-SPECIFIC

Trust is a context-dependent notion. A trust relation in one context does not guarantee its existence in another context.

2) DYNAMIC

Trust is a time-dependent concept. Trusting someone at one point in time does not mean the trust relation will exist at another point in time. Trust relations can change because of new experiences, new behaviours on the part of target users or a shift in interests of either or both users.

3) PROPAGATIVE

'Because of its propagative nature, trust information can be passed from one member to another in a social network, creating trust chains' [12]. As an example, if David trusts Sarah, and Sarah trusts Mathew, there is a trust relation between David and Mathew, whereby David may derive some amount of trust towards Mathew from the strength of the trust relations between David and Sarah, and Sarah and Mathew [12].

4) SUBJECTIVE

Trust is a subjective concept. Being trustworthy in one's mind does not imply a person is considered trustworthy by all others. For instance, suppose David and Sarah are two PhD students in the computer science department, and Mathew is a PhD supervisor and a lecturer in this department. David may believe that Mathew is trustworthy, while Sarah does not. Such differences in opinion arise from people's diverse expectations, biases and interests.

5) ASYMMETRIC

'Trust is typically asymmetric' [12]. In other words, if David trusts Sarah, he may not necessary be trusted by her.

6) EVENT SENSITIVE

Establishing a trust relation may take a great deal of effort and time, but a high-impact event can destroy it [12], [26].

C. COLLECTING TRUST INFORMATION

There are three different sources from which to collect trust information [12]; that is, attitude, experience and behaviour.

1) ATTITUDE

Our attitude is the way we think or feel (positively/negatively) about something. Information about a person's attitude can be captured by their online interactions using a measure such as a Likert scale [12].

2) EXPERIENCE

Experience can refer to the 'knowledge or skill that you get from doing, seeing, or feeling things, or the process of getting this'.[2] In OSNs, users can gain experience information about other users by interacting with them. This experience can be captured by the feedback among users, and better feedback may result in more interactions in future [12].

[2]https://dictionary.cambridge.org/dictionary/english/experience

3) BEHAVIOUR

Human behaviour refers to 'the range of behaviours exhibited by humans . . . [which are] typically influenced by culture, attitudes, emotions, values, ethics, authority, persuasion, coercion and/or genetics' [12], [27]. In OSNs, we may notice a sudden change in the frequency of interaction between two users, or the amount of activity of a user. The first case may indicate that the trust level between those users has decreased. While the second may represent a decline in the user's trust towards the community in which he or she participate [12].

D. ONLINE SOCIAL NETWORKS

Garton *et al.* [28] widely accepted definition concerning OSNs holds that 'when a computer network connects people or organisations, it is a social network. Just as a computer network is a set of machines connected by a set of cables, a social network is a set of people (or organisations or other social entities) connected by a set of social relationships, such as friendship, co-working or information exchange'. OSNs are relatively new and evolving phenomena on the Web. Users of these online platforms can communicate with others and present themselves through their profiles [29], [30].

Social network analysis is an area of study focusing on OSNs that looks for patterns of relations among people [28]. In OSNs, relations can be characterised by their content (i.e., resources exchanged, such as information), direction and strength [28]. One of the relations on which social network analysis focuses is the trust among people in OSNs. These studies aim to understand why people trust each other and establish trust relations in OSNs, with a view to predicting trust relations among people in OSNs.

E. TRUST PREDICTION IN ONLINE SOCIAL NETWORKS

Trust networks in OSNs are usually sparse [25]. They follow the power law distribution whereby a small number of users account for the majority of the trust relations [25]. As a result, the explicit trust relations among many users in OSNs are unknown [13]. Therefore, to employ trust information in different applications in OSNs (e.g., recommender systems and retweet behaviour prediction), we need to predict unknown trust relations among users. Figure 4 illustrates a simple example of the trust prediction procedure; on the left side, we have some users and their explicit trust relations, as shown by the green arrow and the label '1'. We want to know if there is a trust relation between Sarah and John. A trust prediction approach can be used to predict that the existence of this trust relation.

III. TRUST REPRESENTATION

A pair-wise trust relation (Figure 1) is a relationship between a source user (trustor) and a target user (trustee) that indicates that the trustor trusts the trustee. With the help of trust, the trustor may seek information from the trustee, to avoid being confused by the huge amount of available data (i.e., mitigated information overload) and to be confident about

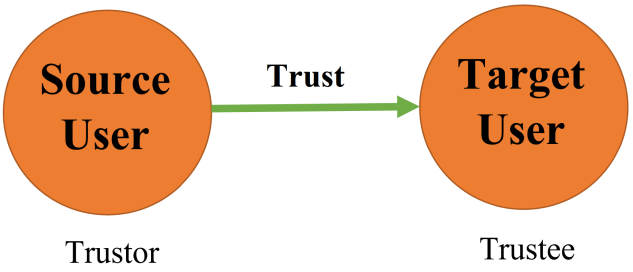


FIGURE 1. Representation of a pair-wise trust relation.

the credibility of the received information (i.e., increased information credibility) [13].

To denote the naivest notion of trust (e.g., single-dimensional trust), one can use a representation similar to Figure 2. In this figure, there are five users (A, B, C, D and E). On the left side, there is a trust network representation among these users, where the green arrow with the label '1', indicates the existence of a trust relation between two users, and its absence means that there is not any trust relation between them. To the right of this figure, there is a corresponding adjacency matrix, showing the trust network between any two users. In this matrix, '0' represents the lack of trust and '1' illustrates the existence of trust between two users.

However, trust may have multiple dimensions. For instance, trust is a context-dependent concept. Context is the information about the condition of an entity [31]. As an illustration of a single context (focusing on the domain of the trust), consider Sarah, a football player, who trusts her coach in football. This does not necessarily mean that she also trusts her coach regarding music. Hence, to represent trust relations among users in different contexts, we need a representation with more dimensions. As another example, if Mathew trusts Jack (as two users in an OSN) at time T_1, this does not necessary mean that Mathew will also trust Jack at time T_2 (where $T_2 = T_1 + h$, and h is a fraction of time). Hence, matrices cannot appropriately represent a multi dimensional trust network. Instead, tensors are one of the most favoured representations for trust relations as they can store data in several dimensions.

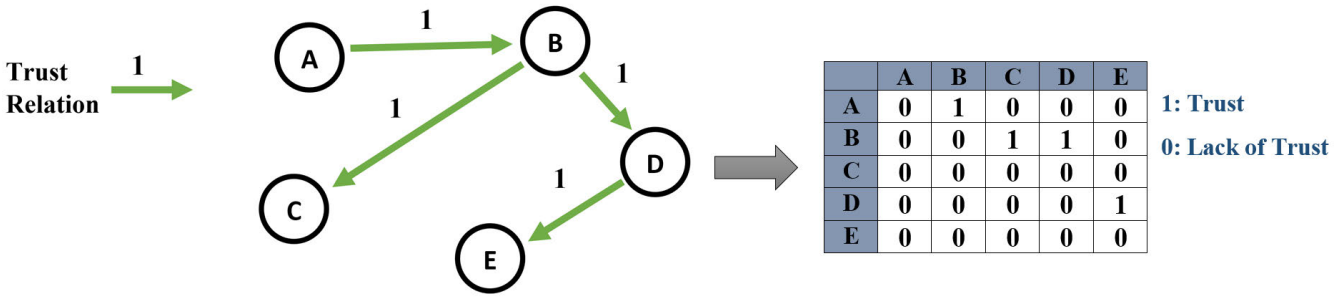
Figure 3 illustrates an example of representing trust relations in different contexts of trust. In this figure, which demonstrates a single dimension of context (e.g., domain of expertise), there are three contexts of trust (football player, computer scientist and plumber). There are also three users (A, B and C). As shown, there are three trust relations between users in the first context (football player). According to these trust relations, A trusts B, B trusts C and C trusts A as a football player. For representing these trusts relations and other trusts relations between these users in other contexts, we can use a tensor. For instance, Figure 3 shows a three dimensional tensor with two dimensions for representing users' relations and a third dimension denoting the contexts of trust. Since all the mentioned trust relations are related to the football player (context 1), they are stored in the matrix of context 1 of this tensor.

IV. CHALLENGES OF TRUST PREDICTION IN ONLINE SOCIAL NETWORKS

This paper will focus on the following three significant problems in OSNs: sparsity of user-specified trust relations, context-aware pair-wise trust relations and time-aware pair-wise trust relations.

A. SPARSITY OF USER-SPECIFIED TRUST RELATIONS

User-specified trust relations are extremely rare [32]. For instance, 'the density of a typical trust network in social media is less than 0.01' [13], [33]. As another example, 'the sparsity of Advogato, Ciao, and Epinions, FriendFeed, and Flixster [frequently used datasets in trust prediction related research], i.e., the ratio of the observed trust relations to all the possible relations, is 0.0011%, 0.0028%, 0.0042%, 0.0041% and 0.0035%, respectively [4], [13], [34], [35]. It is challenging to predict the trust relations well with so limited observed links' [32]. Moreover, trust relations follow the rules of the power law distribution: many trust relations can be accounted for a small number of users and a large number of users participate in only a few trust relations [25]. For any trust prediction approach in OSNs, the number of known user-specified trust relations compared to all possible relations among users is low. This makes the pair-wise trust



	A	B	C	D	E
A	0	1	0	0	0
B	0	0	1	1	0
C	0	0	0	0	0
D	0	0	0	0	1
E	0	0	0	0	0

FIGURE 2. Representation of a trust network and its corresponding adjacency matrix. There are four trust relations in this figure: A trusts B, B trusts C and D, and D trusts E.

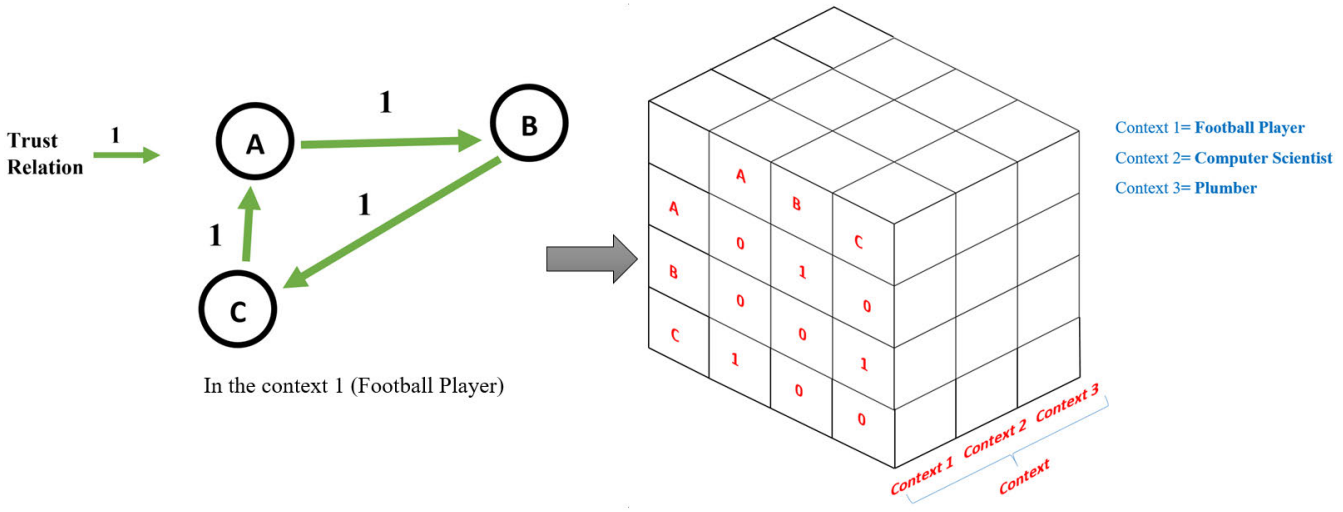


FIGURE 3. Representation of a trust network and its corresponding adjacency tensor. There are three users (A, B and C) and three trust relations and three contexts of trust in this figure: in the first context, A trusts B, B trusts C and C trusts A. Users on rows trust users on columns in this adjacency tensor.

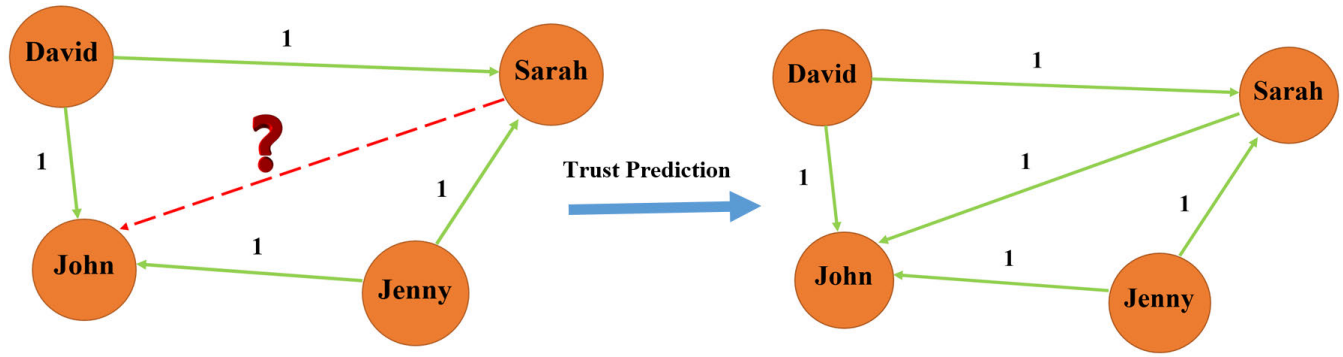


FIGURE 4. Trust prediction in OSNs: David, Sarah, John and Jenny are four users in an OSN. Explicit trust relations are shown by the green arrow and the label '1'. On the left, we want to know if there is any trust relation from Sarah to John. On the right, using a trust prediction model, we can give a positive answer to that question. Sarah trusts John.

prediction problem in OSNs a challenging task; any trust prediction approach should be able to deal with this data sparsity problem.

B. CONTEXT-AWARE PAIR-WISE TRUST RELATIONS

The notion of trust is context-dependent [4], [13]: Trusting someone in one context does not guarantee trusting them in another context [13]. As an example, the context dependency of trust has been investigated by [36] in the collected data from a real-world product review website.[3] In this website there is an option for users to explicitly indicate which users are trustworthy. Tang *et al.* [25] used this information as the ground truth of their analysis. They considered items' categories (e.g., electronics, sports and entertainment) as the context of trust and reported that: 'less than 1% of users, trust their friends in all categories' and 'on average, people trust only 35.4% of their trust networks for a specific category'.

[3]http://www.Epinions.com

Hence, people trust each other in certain contexts. Context is the information about the condition of an entity [31]. As an illustration of a single context (focusing on the domain of the trust), consider David who is a PhD student at the Computing Department. He trusts his supervisor in the computer science field; however, he does not necessarily trust him in sports. As a result, predicting pair-wise trust relations with respect to the different context of trust can be a daunting task.

C. TIME-AWARE PAIR-WISE TRUST RELATIONS

Trust values can also change over time. Users can establish new trust relations or eliminate their existing trust relations after a period of time. For instance, if Jack trusts David (as two users in an OSN) at time T_1, this does not necessary mean that he trusts him at time T_2 (where $T_2 = T_1 + h$ and h is a fraction of time). As another example, David may not trust Sarah at time T_1, but he could trust her at time T_2.

Hence, predicting the pair-wise trust relations statically may not be a realistic approach for OSNs. Trust is time-sensitive: if John trusts David at time T_1, this trust relation may change at time T_2. This can be affected by many factors, such as some new behaviour on David's part or a change in John's interests. Hence, predicting pair-wise trust relations in OSNs dynamically can be a challenging task.

V. TRUST PREDICTION APPROACHES

In this section, we describe related work in four areas: representation of the network, type of prediction algorithms, context-awareness and time-awareness. Finally, we classify the existing pair-wise trust prediction approaches (Table 3).

A. REPRESENTATION OF TRUST NETWORKS

We broadly categorise trust prediction approaches into three categories: graph-based trust models, interaction-based trust models and hybrid trust models [12].

1) GRAPH-BASED TRUST PREDICTION MODELS

Approaches in the category of graph-based trust models are mostly based on the concept of web-of-trust or Friend-of-a-Friend (FOAF). Each user is assumed to have a trust network that contains friends (i.e., social network actors/users) as nodes, with the relationships (i.e., value of their trust relations) among them as the edges [12]. This assumption can be invalid or too strong because, in many online communities, there is either no way to identify a web-of-trust or the connectivity is sparse [37]. Moreover, in some cases, this kind of approach may fail to capture the actual interactions among members [12]. Trust propagation-based [38] and inference-based [39] methods belong to this category.

Golbeck *et al.* [38] proposed another trust inference approach based on the FOAF concept that can determine which pairs of users trust each other and on which topic. Similarly, Zhang *et al.* [40] presented an approach by which the source user accepts the recommendation from similar neighbour nodes (i.e., other users directly connected to the target user). Kim *et al.* [41] proposed an approach to build a web-of-trust based on the implicit feedback of users in a certain context. Golbeck [42] proposed another trust prediction approach, TidalTrust, also based on the FOAF concept. In TidalTrust, if two neighbours have a high trust rating, it is more likely they would agree on other users' trustworthy levels [12]. Ziegler and Lausen [43] developed another network-based trust prediction model, Appleseed, for use in the semantic Web. They focused on local group trust metrics to improve the efficiency of the trust prediction procedure. Hang and Singh [44] introduced a new trust prediction approach based on the similarity of users' trust networks; they treated the recommendation problem as a graph similarity problem [44]. Zuo *et al.* [45] proposed a trust prediction framework based on trust chains and a trust graph. This framework can 'calculate trust along a trust chain and evaluate a trust based on a trust certificate graph' [45]. Caverlee *et al.* [46] developed another trust prediction framework, SocialTrust, focusing on social relationships and users' feedback. SocialTrust also allocates a weight value to feedback according to the PageRank algorithm.

Zhang and Yu [47] designed a semantic-based trust reasoning mechanism for trust prediction in OSNs. They noted that trust is a category-dependent concept and traditional trust prediction approaches required much human effort to predict pair-wise trust relations. They also inferred trust relations by designing a domain ontology and exploiting role-based and behaviour-based reasoning functions [47]. Liu *et al.* [48] proposed a heuristic approach, called the Heuristic Social Context-Aware Trust Network Discovery algorithm, adopting the K-best-first search for addressing the trust network extraction problem by developing a contextual social network structure and proposing the concept of Quality of Trust Network [48]. Azadjalal *et al.* [49] proposed a trust-aware recommendation system and use these trust values to improve the accuracy of their model in present of the sparsity of user-item ratings matrix. They propose a model for identifying implicit trust relations. Moreover, they detect the most prominent users based on the Pareto dominance and confidence concepts to use their opinions in their recommendation model. Guo *et al.* [50] developed a trust-aware recommender system based on a matrix factorization model. Their proposed approach focus on item recommendation rather than rating prediction. They also use the trust values provided by explicit users' feedback. Ghavipour and Meybodi [51] proposed a trust inference method based on aggregation strategy and learning automata. Parvin *et al.* [52] proposed a collaborative filtering recommender system based on users' trust network and ant colony optimization (ACO) algorithm. They ranked users based on social trust relationships and then, using ACO, they assigned proper weight values to users to identify the similarity levels among users. Jiang *et al.* [53] presented a slope one algorithm using trusted data and user similarity for designing a collaborating filtering-based recommender systems. Ruan *et al.* [54] developed a trust inference approach for OSNs using trust's transitivity property. They also proposed a metric for measuring the trust level and its certainty.

2) INTERACTION-BASED TRUST PREDICTION MODELS

Approaches in the previous category may fail to 'capture actual interactions among members. The volume, frequency and even the nature of interaction are important indicators of trust in social networks' [12]. By contrast, interaction-based trust prediction models mainly focus on the interactions among users. Liu *et al.* [37] proposed a classification approach for trust prediction in OSNs based on the action and interactions of users. A similar approach presented by Nepal *et al.* [26] proposed a trust prediction model that considers two types of trust: the trust of other users towards a target user and the trust value that a user has towards a community. Adali *et al.* [55] developed a trust prediction approach focusing on users' communication behaviour and more specifically on conversational trust (i.e., duration and frequency of communication between two users)

and propagation trust. Sacco and Breslin [56] proposed a trust prediction approach centering on the subjective trust values of connected users, based on their social interactions [56]. They stated that most of the existing trust prediction approaches are 'propagating known trust values among peers in a trusted network and do not provide measures for asserting a trust value from user interactions between peers' [56]. These approaches only focus on users' interactions and do not consider the social network structure, which may contain important information about users and the type of relations among them.

3) HYBRID TRUST PREDICTION MODELS

Hybrid trust models combine the network-based and interaction-based models. In particular, they simultaneously consider users' previous interactions and the social network's structure [57]. We proposed a trust prediction model called TDTrust [4]. They proposed a set of context factors for capturing contexts of trust relations among users in OSNs. We also mathematically modeled our trust prediction approach, based on three-dimensional tensor decomposition to consider the context of trust directly in their model and to predict trust relations in different contexts of trust. In another study [58], we proposed a new unsupervised approach, SETTrust, which incorporates the social exchange theory. We proposed that a trust relation can be established if the costs of that relation is less than its benefits. Zhang *et al.* [59] developed a trust link detection scheme. Their approach tens to find subjective trust, reputation, and indirect link between users. They calculate the subjective trust according to the users' previous interactions and assess the users' reputation based on collective objective trust.

B. TYPE OF PREDICTION ALGORITHMS

We now discuss past work from the perspective of the type of algorithms used. We can roughly categorise trust prediction approaches into supervised and unsupervised approaches.

1) SUPERVISED APPROACHES

Liu *et al.* [37] developed a supervised trust prediction model and a classifier that works with a set of users' features and interactions. Ma *et al.* [60] proposed a personalised and cluster-based classification trust prediction model that creates user clusters and then trains a classifier for them. Matsuo and Yamamoto [61] focused on a Japanese e-commerce website called @cosme, and became the first to explain the concept of community gravity: a two-way effect of trust and rating. They followed this with a model to formulate the trust prediction and rating prediction problems. Grana *et al.* [62] introduced a supervised trust prediction approach: a binary classification that focuses on users' reputation. Wang *et al.* [63] proposed a trust-distrust prediction approach that simultaneously employed Dempster-Shafer theory and neural networks. They also analysed the effects of homophily theory, emotion tendency and status theory in trust relations [63]. Zhao and Pan [64] developed another supervised trust prediction approach: a classifier with a feature set that included several trust-related factors. These features could be demographic features (e.g., age and Gender), profile features (e.g., number of follwoers and followees), numeric representation of textual contents provided by users and etc. [65]. They used the existing trust labels for training their classifier. However, the main shortcoming of these approaches is the fact that because of the sparsity of trust relations in OSNs, they have not enough label data available for their training process. Bachi *et al.* [66] developed a new trust inference framework to infer trust-distrust relationships. Their approach was based on frequent subgraph mining, signed networks, social balance theory, edge classification and rule-based link prediction [66]. It decomposed a 'trust network into its ego [4] network components and mining on this ego network set the trust relationships' [66].

Korovaiko and Thomo [68] designed a classifier that works with users' provided ratings on product review websites. They analysed the effects of similarities in users' ratings on their trust relations. Borzymek and Sydow [69] focused on analysing graph-based and users' rating-based attributes and employed a C4.5 decision tree-based algorithm to predict users' trust-distrust relations in OSNs. Lopez and Maag [70] proposed a generic trust prediction framework as a multi-class classifier, employing the RESTful web-service architecture and support vector machines technique [71]. We developed a deep classifier for pair-wise trust prediction in OSNs, called DCAT [65]. They proposed some demographic factors and textual contents-based factors for our classifier. To improve the accuracy of DCAT, they also used the word embeddings of users' textual contents.

Zolfaghar and Aghaie [72] developed a supervised time-aware trust prediction approach. They considered the trust prediction problem as a temporal link prediction problem. Their main focus was analysing historical information on the trust relations (or links). Raj and Babu [73] presented a probabilistic reputation feature model as a supervised trust prediction approach. They proposed a framework using reputation features to solve the cold start problem in trust prediction. They also employed the SMOTE-Boost algorithm to establish balanced classes in their datasets [73]. Zhao *et al.* [74] introduced a trust prediction approach to evaluate the trustworthiness of users and tweets on Twitter, focusing on Twitter data from Latin America. Their approach 'jointly consider users' social and contextual relationships in a Twitter social graph' [74]. Their approach used a novel topic-focused trustworthiness estimator model based on a similarity metric. For instance, if a tweet is similar to trustworthy tweets, it can also be considered trustworthy.

Zhang *et al.* [75] with the aim of addressing the 'all good reputation' problem, proposed a multidimensional trust prediction approach called CommTrust, which evaluated trust by mining users' feedback comments [75].

[4] 'A portion of a social network formed of a given individual,term edego, and the other persons with whom she has a social relationship, termed alters' [67]

Chakraverty *et al.* [76] introduced a logistic regression-based model that focused on the ratings similarity of users to predict their pair-wise trust relations. Their experimental results is somewhat contradict those of Tang *et al.* [25]. Chakraverty *et al.*'s study focused on the implicit similarity and co-rated item-count thresholds, finding low precision, recall and coverage for the similarity threshold and better precision, recall and coverage for the co-rated item-count threshold [76]. Nunez-Gonzalez *et al.* [77] considered the trust prediction problem as a classification problem. They focused on the reputation features of users, because they believed that their reputation information could be used to evaluate the trustworthiness of a user [77]. Raj and Babu [73] proposed a probabilistic reputation feature model to compute the level of trustworthiness in OSNs by identifying the features that determine a user's trustworthiness level.

some researchers focused on employing Bayesian network model in their trust prediction approaches. Denko *et al.* [78] proposed a trust management approach to assess relationships among devices in pervasive computing environments. This approach enables the devices to evaluate the trustworthiness of other devices even if they did not have enough interactions before. Fung *et al.* [79] proposed a Bayesian trust management model for host-based detection system (HIDS) and for tracking the uncertainty in evaluating the HIDS's trustworthiness. Sharma *et al.* [80] presented a trust management framework for pervasive online social networks (POSNs) using concepts of lock door policy and intermediate state management procedure to identify trustworthy and untrustworthy users.

2) UNSUPERVISED APPROACHES

Tang *et al.* [25] proposed an unsupervised trust prediction model called *hTrust*. It exploits the homophily effect on the trust prediction procedure by focusing on similar users. In this way, Tang *et al.* identified similar users based on the users' ratings similarity. They considered three factors for rating similarities: users who rated similar items, users who gave similar ratings for similar items and users who had similar ratings patterns. Wang *et al.* [81] developed an unsupervised model, sTrust, using social status theory and the PageRank algorithm [82], based on *MF*. In this approach, if a user has a higher social status in an OSN, he or she is more likely to be trusted by other users.

Guha *et al.* [83] developed a trust prediction model that propagate trust based on users' trust or distrust relations with others. Golbeck [84] put forward a website called FilmTrust which used trust to produce movie recommendations. Wang *et al.* [32] proposed a trust prediction approach that, in addition to learning low-rank representations of users, also learned these sparse components of the trust network [32]. Zheng *et al.* [31] suggested an unsupervised trust prediction model based on the concept of trust transference, to transfer trust between different contexts [31]. Wang *et al.* [39] introduced an unsupervised trust prediction model to infer trust among users with an indirect connection. Liu *et al.* [85] proposed a trust inference model, incorporating factors such as residential location and outdegree. Wang *et al.* [86] proposed a novel trust prediction model, CATrust, for auction websites, using Bayesian inference based on Markov Chain Monte Carlo. More importantly, their model considered the contexts of trust.

Moradi and Ahmadian [87] proposed a trust-aware recommender system, Reliability-based Trust-aware Collaborative Filtering, to address the problem of the accuracy of ratings predictions in recommender systems. This system dynamically extracts trust networks among users based on similarity values and trust statements. Sanadhya and Singh [88] designed a trust prediction approach based on ant colony optimization (ACO), called Trust-ACO, to calculate trust path and trust cycle and identify the most trustworthy path to find trustworthy services [88]. Their approach is based on probabilistic trust rule, social intimacy pheromone. Fazeli *et al.* [89] proposed a trust prediction approach based on social trust, using *MF*. They first studied the effect of existing trust metrics in predicting pair-wise trust relations, employing those they deemed most effective in their prediction approach.

Massa and Avesani [90] stated that 'predicting a distrust statement is harder than predicting a trust statement'; however, Tang *et al.* [91] have proposed an approach to predict distrust in OSNs. Specifically, their approach facilitates computational understanding of distrust. Zhang *et al.* [92] proposed a context-aware trust prediction approach focusing on 'the ratings of past transactions, the nature of both past transactions and the new transaction' [92]. This approach used transaction context similarities to 'identify and prevent potentially malicious transactions with the value imbalance problem' [92]. Matsutani *et al.* [93] assumed that the trust prediction problem could be solved in the same way as a link prediction problem. They proposed an approach based on non-negative *MF* (NMF) methods. This approach 'incorporates people's evaluation of users' activities as well as trust-links and users' activities themselves' [93].

Tang *et al.* [94] delved into the evolution of trust as a result of interpersonal interactions. They proposed a dynamic MF-based trust prediction approach, called eTrust, which focused on the dynamic preferences of users on product review websites [94]. Huang *et al.* [95] believed that 'people who are in the same social circle often exhibit similar behaviour and tastes'. They treated the trust prediction problem as a link prediction problem and proposed a joint manifold factorisation method that aggregated heterogeneous social networks to explore 'the user group level similarity between correlated graphs and simultaneously [learn] the individual graph structure' [95]. Moturu and Liu [96] proposed an unsupervised approach for evaluating the trustworthiness of shared content, particularly shared health content. They proposed an approach based on feature identification, for determining the features most relevant to trust and quantification. Yao *et al.* [97] proposed a trust inference approach based on *MF*. They addressed the trust prediction problem

as a recommendation problem. Their model 'characterizes multiple latent factors for each trustor and trustee from the locally-generated trust relationships'. To improve the accuracy of their approach, they also employed prior knowledge (e.g., trust bias and trust propagation). Huang *et al.* [98] stated that, since trust matrices are of low-rank, they could consider the trust prediction problem as a recommendation problem. Specifically, they proposed a rank-k matrix completion approach that was robust to noise. Liao *et al.* [99] developed a ranking system for evaluating users' reputation which they used it in evaluating the trust relationships and social acquaintances of users. Su *et al.* [100] developed a trust-aware approach for a reliable personalized Quality of Service (QoS) assessment. They employed a beta reputation system to calculate the reputation of users. Next, they identify similar trustworthy users and finally using user-contributed QoS data of these users, they predict the QoS. Ruan *et al.* [101] proposed a trust-aware approach for increasing the correlation between social media and financial data in the stock market. They collected stock-related data (tweets) from Twitter and they proposed a reputation-based mechanism to identify a firm's Twitter sentiment valence and its stock abnormal returns.

C. CONTEXT-AWARENESS OF TRUST

Existing trust prediction approaches can be classified into two groups based on their consideration of the context of trust: approaches that consider context and those that do not. Before discussing the approaches that fall into these categories, we first discuss the notion of the context of trust as it relates to OSNs.

1) DEFINITION OF CONTEXT

Context, which influences the building of a trust relationship between the trustor and the trustee [102], is multi-faceted [31]. In a society, the interactions between two participants can form a *context* that can provide information such as the time or location of that interaction. Uddin *et al.* [102] provided a definition for context of trust in OSNs: 'a context is a situation, which influences in the building of a trust relationship between the trustor and the trustee'.

2) CONTEXT-LESS APPROACHES

The context-less approaches do not consider context to predict a trust relation in OSNs. The majority of existing trust prediction approaches can be considered context-less (see Tang *et al.* [25], Wang *et al.* [81], Golbeck [84] and Wang *et al.* [32]). These approaches assume that if John trusts Jack, this means John trusts Jack in all fields of expertise (e.g., electronics, sports, music, movies and science), for a lifetime and in any location. This assumption is too simplistic for real-word scenarios, because people only trust each other in certain contexts [4], [13], [36].

3) CONTEXT-AWARE APPROACHES

Liu *et al.* [103] and Zhang and Wang [104] highlighted the importance of the context of trust as an essential factor for trust prediction approaches. However, little effort has been made to consider the context of trust for a first class citizen. One exception is Zheng *et al.* [31], who proposed a context-aware approach that considers both user's properties and the features of contexts. Social trust proposed as a novel probabilistic social context-aware trust inference approach, exploits textual information to deliver better results [39]. In Zheng *et al.*'s approach, trust is inferred along the paths connecting two users. Thus, if two users are not connected by any path, no trust among them can be predicted. Similarly, Liu *et al.* [85] developed a context-aware trust prediction approach based on the web-of-trust concept, which considered social context factors, such as users' location, previous interactions, social intimacy degree with other users, existing trust relations and so on. Zolfaghar and Aghaie [105] proposed a supervised context-aware trust prediction approach. They investigated the effects on trust relations of certain social trust factors, such as contextual similarity, users' reputation and relationship-based trust factors.

Zhang *et al.* [106] proposed a novel context-aware trust prediction approach based on contextual transaction factors, categorised into those relating to service and those relating to transaction [106]. This approach considered the context of past transactions and forthcoming transactions to evaluate the reputation profile of the seller [106]. In another study, Zhang *et al.* [107] aimed to develop a context-aware trust prediction approach. They designed a data structure to support the Contextual Transaction Trust (CTT) computation in e-commerce environments [107]. They also proposed 'an approach for promptly responding to a buyer's CTT query' [107]. Liu *et al.* in [108], [109] and [110] noted that 'predicting the trust between two unknown participants based on the whole large-scale social network can lead to very high computation costs' [108]. Hence, they proposed an approach to extract a sub-network of the trust network that contained the most important nodes and trust relations. Since this sub-network extraction problem is a NP-complete problem, they proposed a strong social component-aware trust sub-network extraction model, So-BiNet, to address this [108]. Zheng *et al.* [111] proposed another solution to 'extract a small-scale contextual network that contains most of the important participants as well as trust and contextual information' [111]. They developed a context-aware trust sub-network extraction model. They also used ant colony algorithm sub-network extraction.

Liu and Datta [112] introduced a new context-aware trust prediction approach based on the Hidden Markov Model (HMM). This approach can dynamically model a user's interactions in OSNs. Rettinger *et al.* [113] proposed a context-aware trust prediction approach, called the Infinite Hidden Relational Trust Model. They expressed that 'from the truster's point of view trust is best expressed as one of several relations that exist between the agent to be trusted (trustee) and the state of the environment'. Xiong and Liu [114] developed a novel context-aware trust prediction model, PeerTrust, for e-commerce platforms, based on

a transaction-based feedback system. They also introduced the factors of transaction context and community context for capturing the contexts of trust relations. Rehak *et al.* [115] designed a situational (context-dependent) trust prediction approach. They proposed a mechanism that 'describes the similarity among the situations using their distance in a metric space and defines a set of reference contexts in this space to which it associates the trustfulness data'.

Uddin *et al.* [102] proposed an interaction-based context-aware trust prediction approach, called CAT. They also suggested the concept of context similarity, which can be used for decision making in similar situations [102]. Kim *et al.* [41] believed that existing trust prediction approaches mostly relied on the web-of-trust concept, which may fail to accurately predict trust relations among users because of the data sparsity problem. They developed a context-aware trust prediction approach focusing on users' expertise and affinity in a particular context (topic). Li and Wang [116] developed a fuzzy comprehensive evaluation based method to evaluate the trustworthiness of a service provider in an upcoming transaction based on the trust ratings in its transaction history. This approach is grounded in context-based trust normalisation, which focuses on 'the familiarity between each rater and the service client of the upcoming transaction' [116]. Wu *et al.* [117] proposed a linguistic trust model for direct trust relations of group experts in social network group decision making (SN-GDM) using trust/distrust values. Then, they combined the social network trust with the collaborative filtering to propose a comprehensive estimation method for incomplete information. Burt *et al.* [118] analyzed the well-being, business differences, political views and demographic features of users in the strong ties known in China as guanxi. Their finding illustrate that there is a strong relationship between trust and social network and '' Trust variance is 60% network context, and 10% individual differences''. Li *et al.* [119] designed a context-aware and trust-aware recommendation based on Gaussian mixture model (GMM). Their assumed that decisions and preferences of users may be affected by their trusted friends.

D. TIME-DEPENDENCY OF TRUST

Although time can be considered one of the elements of context, because of its importance we investigate it more deeply. The literature on time-aware trust prediction in OSNs can be divided into two categories based on the approach taken: static approaches and dynamic approaches.

1) STATIC TRUST PREDICTION APPROACHES

Static trust prediction approaches assume that trust relations among users do not change over time. However, in real-world scenarios, trust relations among people may be terminated at any time for various reasons (e.g., changes in interests, expectations or opinions). The majority of existing trust prediction approaches belong to this category (see Liu *et al.* [37], Ma *et al.* [60], Matsuo and Yamamoto [61], Tang *et al.* [25], Wang *et al.* [81] Ghafari *et al.* [4], [58] and Wang *et al.* [32]).

2) DYNAMIC TRUST PREDICTION APPROACHES

Dynamic trust-prediction approaches can be classified into three main categories: Beta models, HMM-based models and others.

In the Beta models, Beta probability density functions consider reputation and feedback simultaneously (see Ismail and Josang [120]). In another work [121], a decay factor was used to give more weight to recent events based on Recency bias (i.e., a person will remember the most recent events more easily compared to older events). Zhang and Cohen [122] introduced an approach that monitors the dynamic behaviour of an agent based on the concept of time windows. In each time window, the number of successful and unsuccessful transactions is considered.

HMM-based models use HMM to propose dynamic trust prediction models. These approaches are of two main types. The first type focuses on the outcomes of past transactions and observations of HMM [16], [123], [124]. Although these may have better performance compared to the Beta models, they fail to consider contextual information about each transaction [16]. In the second type, researchers seek to consider contextual information about the transactions (see Liu and Datta [112]). Zheng *et al.* [125] developed a dynamic trust prediction approach based on HMM, which focused on the hidden characteristics of the HMM model as well as the outcomes. They used a service provider's historical transactions to predict its trust level. They considered 'static features, such as the provider's reputation and item price and the dynamic features, such as the latest profile changes of a service provider and price changes' [125]. Malik *et al.* [126] presented a means of assessing reputation in a service oriented approach for service oriented environments based on HMM. This approach can predict trust-based interactions among Web services.

Falling under the third category of dynamic trust prediction approaches, Cai *et al.* [127] proposed a MF-based trust prediction model. They incorporated temporal dynamics to model the dynamics of users' preferences. Laifa *et al.* [128] tested a research model using structural equation modeling and delivered the outputs to an artificial neural network and fuzzy logic model developing their dynamic prediction approach. Liu and Datta [129] designed another dynamic trust prediction approach. They believed that modelling the behaviour of people is challenging as people may change their behaviour strategically to increase their profits [129]. By measuring similarity among the contexts of transactions, they estimated the trustworthiness of a transaction based on previous cases of similar transactions. Although these approaches give outstanding performance in some situations, they may fail when a user's 'behaviour is highly dynamic or is changing strategically' [16].

E. PERSONALITY AND TRUST

Alarcon *et al.* [130], in investigating the relation between personality and trust, focused on the relations between

propensity to trust, the five-factor model [131], trust beliefs and behaviours. Thielmann and Hilbig [132] researched the impact of HEXACON, another trait-based personality mechanism, on trustworthiness by designing three trust games. Their work demonstrated the relation between honesty/humility and trustworthiness, independent of the prior level of trust. Another study by Evans and Revelle [133] considered the trust inventory and personality traits and validated this inventory through an economic task. They discovered that trust can be related to the Extraversion personality trait. Sicora [134] focused on trust among co-workers and workplace leaders and its relationship with two personality models. Their aim was to create greater trusting relationships in organisations [134]. Gerris *et al.* [135] studied the influence of the Big Five personality traits of couples on their marriages. Solomon *et al.* [136] studied Twitter users based on the Big Five personality model [131] and the Schwartz sociological behaviour model [137] to understand the psycho-sociological homophilic nature of personal networks. We proposed a pattern-based word embedding technique, personality2vec [138] as a novel data analytics pipeline that enables analysis of users' personality patterns and behavioural disorders, based on their activities in OSNs. We also proposed to use domain knowledge to design cognitive services to automatically contextualise raw social data and prepare them for behavioural analytics.

Although there are a rich body of knowledge in the literature of trust related studies in psychology of social science, unfortunately researchers do not pay attention to focusing on the personality traits of users to evaluate their trust relations. Considering users' personality traits could be a good direction for future researches in this domain.

VI. EVALUATION METRICS FOR TRUST PREDICTION PROCESS

In this section, we discuss the evaluation metrics that are frequently used in trust prediction approaches.

A. RANKING-BASED EVALUATION

One of the most well-known trust prediction evaluation metrics is ranking-based evaluation [13], [25], [81]. For this evaluation metric, we divide each of our datasets into two parts. The first part includes users who do not have any trust relations (N). The second part includes users who have trust relations with other users (T). We sort these trust relations based on their time of establishment. At that point, we select the first $A\%$ trust relations as old trust relations and denote $1-A\%$ of them as the *New* trust relations to predict. We consider four percentage values for A={60,70,80,90}. Further, we employ a trust prediction metric from Liben-Nowell and Kleinberg [139] to evaluate the performance of our approaches. Based on this, we first merge all *New* (new trust relations) and N (non-trust relations) such that $N \cup New$ and call them M. Then, we predict the trust relations in M and extract the $|New|$ number of trust relations and call this *Predict*. Based on these sets, the performance of any trust prediction approach is determined by the following formula:

$$TPA = \frac{|New \cap Predict|}{|New|} \tag{1}$$

where *TPA* is the trust prediction quality. The value of *TPA* is usually small and 'to demonstrate the significance of performance, [a] randomly guessing predictor is usually used as a baseline method' [13]. As we increase the size of A, the size of *New* decreases. This makes it difficult to accurately predict trust relations in M; thus, the *TPA* is expected to decrease.

B. THE MEAN ABSOLUTE ERROR AND ROOT MEAN SQUARED ERROR METRICS

Two widely used prediction accuracy metrics for trust prediction approaches are mean absolute error (MAE) and root mean squared error (RMSE) [4], [13], [65]. Similar to the settings for the ranking based metric, we create M, *New* and N. Then, the trust values for the pairs of users in N are computed. MAE and RMSE can be defined as follows:

$$MAE = \frac{1}{|New|} \sum_{i,j \in New} |T_{AC_{ij}} - T_{Pre_{ij}}|, \tag{2}$$

$$RMSE = \sqrt{\frac{1}{|New|} \sum_{i,j \in New} (T_{AC_{ij}} - T_{Pre_{ij}})^2} \tag{3}$$

where $T_{AC_{ij}}$ is the actual trust relations between u_i and u_j, and $T_{Pre_{ij}}$ is the predicted trust relations. A lower MAE and RMSE indicate a better performance. A small improvement in terms of RMSE or MAE has a significant effect on the quality of the top-few recommendations [13].

C. PRECISION, RECALL AND F1 SCORE

In the field of machine learning and classification problems, there is a matrix called "Confusion matrix" or "error matrix" is used to evaluate the performance of algorithms (Table 1). Obviously, results with the true positive and true negative labels are the desired results. Based on this matrix, Precision and Recall metrics can be defined as follows:

$$Precision = \frac{TruePositive}{TruePositive + FalsePositive} \tag{4}$$

$$Recall = \frac{TruePositive}{TruePositive + FalseNegative} \tag{5}$$

where Precision is the percentage of relevant results compared to the retrieved results, while Recall is the percentages of relevant instances that were successfully retrieved. Finally, F1 measure is combining both Precision and Recall as follows:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{6}$$

TABLE 1. The confusion matrix.

Confusion Matrix	
True Positive	False Positive
False Negative	True Negative

TABLE 2. Datasets that researchers are frequently used for evaluating trust prediction approaches.

Dataset	Number of users	Trust network density	Number of trust relations
Epinions [81] [25]	8,527	0.0042	302177
Ciao [81] [25]	6,262	0.0028	109524
Advogato [32]	6541	0.0011	51127
FriendFeed [34]	4148	0.0041	386,804
Flixster [35]	6072	0.0035	167552
Wiki-RfA [140]	10835	0.0013	159388
Wiki-Elec [141]	7115	0.0020	103689

VII. DATASETS FOR TRUST PREDICTION APPROACHES

In this section, we introduce the datasets that researchers are frequently used for evaluating their proposed trust prediction approaches. In most of these datasets, each pair of users has a Boolean label associated with its trust relation (which acts as the ground truth for our experiments). For instance, in the Epinions and Ciao Datasets [25], [81], the trust labels are generated by explicitly asking users to give a '0' or '1' value as the trust value to other users. Epinions and Ciao Datasets also contain the attributes of the users and their reviews, and use a 5-star (one-to-five) rating system to rate reviews. The reviews in these datasets are categorised by topic, such as travel, books, food and drink, house and garden and family. In addition to the Epinions and Ciao datasets, Table 4 summarize the characteristics of other datasets that researchers can use in their evaluations. In this table, trust network density represents the ratio of the number of known trust relations and the possible trust relations (number of users $\times$ (number of users-1)).

Advogato dataset is crawled from Advogato.org website which is for development of open-source software. Similar to Epinion and Ciao, the users in Advogato can explicitly certify other users as ''observer'', ''apperentice'',''journeyer'' and ''master'' which can demostrate the level of trustworthy of a user. Flixster and FriendFeed also are similar to the Epinions and Ciao datasets and users can provide a rating for other users' feed using a 5-star (one-to-five) rating system. Moreover, Wiki-RfA and Wiki-Elec datasets are based on the the votes that Wikipedia members are providing for an editor in Wikipedia to become an administrator.[56]

VIII. ANALYSIS

In this Section, we first have an analysis over the existing trust prediction approaches from the point of view of their structures. Next, we compare the current approaches with respect to their time complexity.

A. ANALYZING THE EXISTING TRUST PREDICTION APPROACHES

To gain a better understanding of the existing trust prediction approaches, in Table 3 we classify the existing approaches according to whether they are supervised (S) or unsupervised (U), where S denotes supervised and U represents unsupervised; whether the context of trust is considered, where Y represents that the property is satisfied and N denotes that the method cannot satisfy the property; and whether the dynamic, time-dependent nature of trust is considered, where Y likewise denotes that the property is satisfied, while N means it is not. Based on this analysis, we find that around 54% of existing trust-prediction approaches do not consider the context of trust. This means, they assume all trust relations are the same and that if a user trusts another user in one context, he or she will trust that user across all contexts. Surprisingly, only 27% of existing trust-prediction approaches are time-aware. Accordingly, the majority of existing approaches assume that trust relations last a lifetime.

B. TIME COMPLEXITY

In this subsection, we compare different trust prediction approaches from the point of view of their time complexity. Here, we mainly focused on the trust prediction approaches that discussed the time complexity of their approaches explicitly, or at least they provided the algorithms of their models. Table 4 compare these approaches.

IX. FUTURE DIRECTIONS

In this paper, we have investigated the problem of predicting trust between two unknown users in OSNs. We believe this is an important research area that has important applications for business and government in understanding trends in the diffusion of misinformation on OSNs. We believe this important research area, will attract a great deal of attention from the research community over the coming years. Below, we summarise some significant research directions in this area.

A. CONTEXT AND DATA CURATION

Although several context-aware trust prediction approaches have been proposed in the literature, there remains room to study the factors that can accurately capture the context of trust relations. It would be useful to investigate the use of textual contents in trust prediction approaches. As an almost unexplored research topic in trust prediction area, researchers need to use natural language processing techniques [142] to analyse textual contents as a rich source of information about users' activities and behaviour. Such analysis would enrich our available data about users and their relations, potentially helping to alleviate the data sparsity problem.

Accordingly, understanding the content and context of social data can help in understanding the trust relations among users in OSNs. For example, if a user retweets a

[5]http://snap.stanford.edu/data/wiki-RfA.html
[6]http://snap.stanford.edu/data/wiki-Vote.html

TABLE 3. Classification of existing trust prediction approaches: are they supervised (S), unsupervised (U), context-aware, and time-aware (dynamic)?.

Approach	Supervised/Unsupervised	Context-Aware	Dynamic
Moradi and Ahmadian [87]	U	N	Y
Sanadhy and Singh [88]	U	N	Y
Raj and Babu [73]	U	N	N
Zhao et al. [74]	S	Y	N
Zhang et al. [92]	U	Y	Y
Zhang et al. [106]	S	Y	N
Zhang et al. [75]	S	N	N
Zhang et al. [107]	S	Y	N
Liu et al. [108]	U	Y	N
Zheng et al. [111]	U	Y	N
Matsutani et al. [93]	U	N	N
Tang et al. [94]	U	N	Y
Zhang and Yu [47]	U	N	N
Chakraverty et al. [76]	S	N	N
Sacco and Breslin [56]	S	N	N
Huang et al. [95]	U	N	N
Li and Wang [116]	U	Y	N
Fazeli et al. [89]	U	N	N
Tang et al. [91]	U	N	N
Moturu and Liu [96]	U	N	N
Nunez-Gonzalez et al. [77]	S	N	N
Yao et al. [97]	U	N	N
Huang et al. [98]	U	N	N
Liu et al. [37]	S	N	Y
Ma et al.L [60]	S	N	N
Matsuo and Yamamoto [61]	S	N	Y
Grana et al. [62]	S	N	N
Wang et al. [63]	S	N	N
Bachi et al. [66]	S	Y	N
Korovaiko and Thomo [68]	S	N	N
Borzymek and Sydow [69]	S	N	N
Laspez and Maag [70]	S	Y	N
Ghafari et al. [65]	S	Y	N
Zolfaghar and Aghaie [72]	S	Y	Y
Tang et al. [25]	U	N	N
Wang et al. [81]	U	N	N
Ghafari et al. [58] and [4]	U	Y	N
Guha et al. [83]	U	N	N
Golbeck [84]	U	N	N
Wang et al. [32]	U	N	N
Zheng et al. [31]	U	Y	N
Wang et al. [39]	U	Y	N
Liu et al. [85]	U	Y	N
Wang et al. [86]	U	Y	Y
Liu et al. [103]	U	Y	N
Zhang and Wang [104]	U	Y	N
Zolfaghar and Aghaie [105]	S	Y	N
Liu and Datta. [112]	S	Y	Y
Rettinger et al. [113]	S	Y	N
Xiong and Liu [114]	U	Y	N
Rehak et al. [115]	S	Y	Y
Uddin et al. [102]	U	Y	Y
Kim et al. [41]	U	Y	N
Ismail and Josang [120]	U	N	N
Teacy et al. [122]	U	N	Y
Moe et al. [124]	S	N	Y
Elsalamouny et al. [123]	S	N	Y
Zheng et al. [125]	S	Y	Y
Malik et al. [126]	U	N	Y
Liu and Datta [129]	U	Y	Y
Laifa et al. [128]	S	Y	N
Golbeck [38]	U	N	N
Trifunovic et al. [57]	U	N	N
Zhang et al. [40]	U	N	N
Kim et al. [41]	U	Y	N
Ziegler and Lausen [43]	S	Y	N
Hang and Singh [44]	U	N	N
Zuo et al. [45]	U	N	N
Caverlee and Liu [46]	U	Y	Y
Liu et al. [48]	U	Y	Y

TABLE 4. Time complexity of trust prediction approaches. *n* is the number of users.

Approach	Time Complexity
Sanadhy and Singh [88]	n^2A, where A is the number of ants
Zhao et al. [74]	n^2
Zhang et al. [92]	n^2
Zhang et al. [107]	nlogn
Zheng et al. [111]	n^2
Tang et al. [91]	n^2d, where d is the number of iterations before reaching the converged state
Yao et al. [97]	$nm + \|K\|m$, where K and m are the number of trust relations and algorithm's maximum iteration number
Huang et al. [98]	nd, where d is the number of iterations before reaching the converged state
Bachi et al. [66]	n
Laspez and Maag [70]	n^2
Ghafari et al. [65]	n^3
Tang et al. [25]	n^2d, where d is the number of iterations before reaching the converged state
Wang et al. [81]	n^2d, where d is the number of iterations before reaching the converged state
Ghafari et al. [58] and [4]	n^2d, where d is the number of iterations before reaching the converged state
Wang et al. [39]	n^2
Liu et al. [85]	$n\lambda$, where λ is the maximal search hops
Wang et al. [86]	kn_rn_n, where n_r, n_n and k are the number of nodes, services per node, and the number of iterations for convergence state
Liu et al. [103]	mld, where m, l and d are the number of simulations, the average length of trust paths and the maximal outdegree of nodes.
Moe et al. [124]	n^2
Liu and Datta [129]	$NS - S^2$, where N is the umber of past transactions, S is the transaction window's size.
Trifunovic et al. [57]	n^2d, where d is the number of iterations before reaching the converged state
Ziegler and Lausen [43]	n^2
Liu et al. [48]	$Km\lambda$, where K, m and λ are the number expansion nodes at each hop, the maximal outdegree, and the maximal search hops

tweet on Twitter, it would be helpful to understand the text of the tweet, whether it contains an image or URL, and the keywords or entities (e.g., people, organisations, locations and products) and topics mentioned. In this context, data curation [143]–[145] (i.e., the task of preparing the raw data for analytics) can help in turning raw data into contextualised data and knowledge. For example, curating a raw tweet from Twitter can tell us if the tweet contains a mention of a person named Barak Obama (using entity extraction and coreference reolution techniques [146]) who was the 44th president of the United States (using linking techniques [147] to link this entity to external knowledge sources such as Wikidata [7]). We can also understand if the topic of the tweet is related to politics (using topic extraction [148]) and if the tweet is discussing a social issue (using rule-based techniques [149]). A future direction would be to use data curation in OSNs to improve the accuracy of predicting the trust relation between two users.

B. TIME AND BUSINESS PROCESSES

Although there were a few attempts to introduce novel time-aware trust prediction approaches that can dynamically predict trust relations, the time complexity of these approaches in real-world scenarios must be critically examined. In other words, the next trust prediction approaches should focus on decreasing the execution times. Many of the existing trust prediction models are based on a computationally complex model with a high execution time. By decreasing the execution time of trust prediction approaches, we make them more feasible for real-world applications.

An important application in this category is to understand customer's personality, behaviour and attitude in business processes [150], [151] and to predict how their trust in companies and products may change over time. Business processes are a set of tasks and activities performed to accomplish a specific organisational goal [152], [153]. For example, consider a bank customer who has decided to change their bank or a specific product offered by a bank. Analysing the time-aware activities of bank customers may allow the loss of a trust relation for an existing product to be predicted. Another interesting avenue for future work in this domain would be to use data provenance [154], [155] to model and understand the evolution of social items over time. For example, to help predict customers' personality, behaviour and attitude in business processes, their retweets, likes and views could be analysed over time [138].

C. BENCHMARKING DATASETS

Surprisingly, even after several years of research in the trust prediction area, researchers still suffer from an absence of test datasets that provide sufficient contextual information about users and the dynamic timestamp of their trust relations. As an urgent need in this domain, providing such a dataset for trust prediction related research could help to attract many more researchers to this research area. Future work in this domain would be to use crowdsourcing techniques [156]–[158] to facilitate the labelling of such datasets.

D. CONTINUOUS TRUST METRICS

Although most of the existing trust prediction approaches assume that trust is a binary concept ("0" for lack of a trust relation and and "1" for a trust relation between a pair of users), in real-word scenarios the trust relations can be Continuous variables and assign any real numbers as trust values [13]. In the future, researcher could more focus on this area of research. However, they employ the right evaluation

[7] https://www.wikidata.org/

metrics and datasets (relevant for Continuous trust values) in their evaluations.

X. CONCLUDING REMARKS

OSNs enable users to connect with others, expand their social networks, share multimedia content and write reviews on specific items. Users in OSNs are bombarded with information and trust can play an important role in their decision making. Due to the lack of interactions between the majority of participants on OSNs, predicting pair-wise trust relations in this context is a daunting task. In this paper, we extensively analysed the concept of trust and presented three main research challenges related to the trust prediction process. Next, we classified the state-of-the-art trust prediction approaches based on addressing those challenges. Finally, we suggested some potential research directions for researchers in this field.

REFERENCES

[1] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, Jul. 1995.
[2] N. Luhmann, *Trust Power*. Chichester, U.K.: Wiley, 1979.
[3] Z. Li, X. Zhang, H. Shen, W. Liang, and Z. He, "A semi-supervised framework for social spammer detection," in *Advances in Knowledge Discovery and Data Mining, PAKDD*. Hanoi, Vietnam: Springer, 2015, pp. 177–188.
[4] S. M. Ghafari, A. Beheshti, S. Yakhchi, and M. Orgun, "Social context-aware trust prediction: A method for identifying fake news," in *Proc. 19TH WISE*, 2018, pp. 161–177.
[5] D. R. Bild, Y. Liu, R. P. Dick, Z. M. Mao, and D. S. Wallach, "Aggregate characterization of user behavior in Twitter and analysis of the retweet graph," *ACM Trans. Internet Technol.*, vol. 15, no. 1, pp. 1–24, Mar. 2015.
[6] N. A. Abdullah, D. Nishioka, Y. Tanaka, and Y. Murayama, "Why i retweet? Exploring User's perspective on decision-making of information spreading during disasters," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 1–10.
[7] X. Ma, H. Lu, and Z. Gan, "Implicit trust and distrust prediction for recommender systems," in *Proc. Int. Conf. Web Inf. Syst. Eng.*, 2015, pp. 185–199.
[8] Y. Yu, Y. Gao, H. Wang, and R. Wang, "Joint user knowledge and matrix factorization for recommender systems," in *Proc. 17th Int. Conf. Web Inf. Syst. Eng. WISE*, 2016, pp. 77–91.
[9] A. Caliò and A. Tagarelli, "Complex influence propagation based on trust-aware dynamic linear threshold models," *Appl. Netw. Sci.*, vol. 4, no. 1, p. 14, Dec. 2019.
[10] B. Abu-Salih, K. Y. Chan, O. Al-Kadi, M. Al-Tawil, P. Wongthongtham, T. Issa, H. Saadeh, M. Al-Hassan, B. Bremie, and A. Albahlal, "Time-aware domain-based social influence prediction," *J. Big Data*, vol. 7, no. 1, p. 10, Dec. 2020.
[11] S. Liu, L. Zhang, and Z. Yan, "Predict pairwise trust based on machine learning in online social networks: A survey," *IEEE Access*, vol. 6, pp. 51297–51318, 2018.
[12] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 1–33, 2013.
[13] J. Tang and H. Liu, *Trust Social Media*. San Rafael, CA, USA: Morgan & Claypool, 2015.
[14] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.
[15] B. R. Schlenker, B. Helm, and J. T. Tedeschi, "The effects of personality and situational variables on behavioral trust.," *J. Personality Social Psychol.*, vol. 25, no. 3, pp. 419–427, 1973.
[16] X. Zheng, "Trust prediction in online social networks," Ph.D. dissertation, Dept. Comput., Macquarie Univ., Sydney, NSW, Australia, 2015.
[17] P. Sztompka, *Trust: A Sociological Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[18] L. G. Zucker, "Production of trust: Institutional sources of economic structure," *Res. Organizational Behav.*, vol. 8, no. 1, pp. 53–111, 1986.
[19] A. B. Seligman, *The Problem Trust*. Princeton, NJ, USA: Princeton Univ. Press, 2000.
[20] S. Jones, *TRUST-EC: Requirements for Trust Confidence E-Commerce*. Brussels, Belgium: European Commission, Joint Research Center, 1999.
[21] R. M. Morgan and S. D. Hunt, "The commitment-trust theory of relationship marketing," *J. Marketing*, vol. 58, no. 3, pp. 20–38, Jul. 1994.
[22] S. Ba and P. A. Pavlou, "Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior," *MIS Quart.*, vol. 26, no. 3, pp. 243–268, 2002.
[23] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "Shiny happy people building trust?: Photos on e-commerce websites and consumer trust," in *Proc. Conf. Hum. Factors Comput. Syst. CHI*, 2003, pp. 121–128.
[24] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic Web," *J. Web Semantics*, vol. 5, no. 2, pp. 58–71, Jun. 2007.
[25] J. Tang, H. Gao, X. Hu, and H. Liu, "Exploiting homophily effect for trust prediction," in *Proc. 6th ACM Int. Conf. Web Search Data Mining WSDM*, 2013, pp. 53–62.
[26] S. Nepal, W. Sherchan, and A. Bouguettaya, "A behaviour-based trust model for service Web," in *Proc. IEEE Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Dec. 2010, pp. 1–4.
[27] R. G. Golledge and R. J. Stimson, *Spatial Behavior: A Geographic Perspective*. New York, NY, USA: Guilford Press, 1997.
[28] L. Garton, C. Haythornthwaite, and B. Wellman, "Studying online social networks," *J. Comput.-Mediated Commun.*, vol. 3, no. 1, Jun. 2006, Art. no. JCMC313.
[29] R. Gross, A. Acquisti, and H. J. Heinz, "Information revelation and privacy in online social networks," in *Proc. ACM Workshop Privacy Electron. Soc. WPES*, 2005, pp. 71–80.
[30] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: Why we disclose," *J. Inf. Technol.*, vol. 25, no. 2, pp. 109–125, Jun. 2010.
[31] X. Zheng, Y. Wang, M. A. Orgun, G. Liu, and H. Zhang, "Social context-aware trust prediction in social networks," in *Proc. ICSOC*, 2014, pp. 527–534.
[32] X. Wang, Z. Zhang, J. Wang, P. Cui, and S. Yang, "Power-law distribution aware trust prediction," in *Proc. 27th Int. Joint Conf. Artif. Intell.*, Jul. 2018, pp. 3564–3570.
[33] R. Zafarani, M. A. Abbasi, and H. Liu, *Social Media Mining: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2014.
[34] L. Chen and J. Gao, "A trust-based recommendation method using network diffusion processes," 2018, *arXiv:1803.08378*. [Online]. Available: https://arxiv.org/abs/1803.08378
[35] X. Wang, Y. Liu, G. Zhang, F. Xiong, and J. Lu, "Diffusion-based recommendation with trust relations on tripartite graphs," *J. Stat. Mech., Theory Exp.*, no. 8, 2017.
[36] J. Tang, H. Gao, and H. Liu, "MTrust: Discerning multi-faceted trust in a connected world," in *Proc. 5th ACM Int. Conf. Web Search Data Mining WSDM*, 2012, pp. 93–102.
[37] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim, "Predicting trusts among users of online communities: An epinions case study," in *Proc. 9th ACM Conf. Electron. Commerce EC*, 2008, pp. 310–319.
[38] J. Golbeck, B. Parsia, and J. A. Hendler, "Trust networks on the semantic Web," in *Proc. CIA*, 2003, pp. 238–249.
[39] Y. Wang, L. Li, and G. Liu, "Social context-aware trust inference for trust enhancement in social network based recommendations on service providers," *World Wide Web*, vol. 18, no. 1, pp. 159–184, Jan. 2015.
[40] Y. Zhang, H. Chen, and Z. Wu, "A social network-based trust model for the semantic Web," in *Proc. ATC*, 2006, pp. 183–192.
[41] Y. Ae Kim, M.-T. Le, H. W. Lauw, E.-P. Lim, H. Liu, and J. Srivastava, "Building a Web of trust without explicit trust ratings," in *Proc. IEEE 24th Int. Conf. Data Eng. Workshop*, Apr. 2008, pp. 531–536.
[42] J. A. Golbeck, "Computing and applying trust in Web-based social networks," Ph.D. dissertation, Dept. Comput., Univ. Maryland, College Park, MD, USA, 2005.
[43] C.-N. Ziegler and G. Lausen, "Spreading activation models for trust propagation," in *Proc. IEEE Int. Conf. e-Technol., e-Commerce e-Service*, Mar. 2004, pp. 83–97.
[44] C.-W. Hang and M. P. Singh. (2010). *Trust-Based Recommendation Based on Graph Similarity*. [Online]. Available: http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf

[45] Y. Zuo, W.-C. Hu, and T. O'Keefe, "Trust computing for social networking," in *Proc. 6th Int. Conf. Inf. Technol., New Generat.*, Apr. 2009, pp. 1534–1539.

[46] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: Tamper-resilient trust establishment in online communities," in *Proc. 8th ACM/IEEE-CS joint Conf. Digit. Libraries JCDL*, 2008, pp. 104–114.

[47] Y. Zhang and T. Yu, "Mining trust relationships from online social networks," *J. Comput. Sci. Technol.*, vol. 27, no. 3, pp. 492–505, Jan. 2012.

[48] G. Liu, Y. Wang, M. A. Orgun, and H. Liu, "Discovering trust networks for the selection of trustworthy service providers in complex contextual social networks," in *Proc. IEEE 19th Int. Conf. Web Services*, Jun. 2012, pp. 384–391.

[49] M. M. Azadjalal, P. Moradi, A. Abdollahpouri, and M. Jalili, "A trust-aware recommendation method based on Pareto dominance and confidence concepts," *Knowl.-Based Syst.*, vol. 116, pp. 130–143, Jan. 2017.

[50] G. Guo, J. Zhang, F. Zhu, and X. Wang, "Factored similarity models with social trust for top-N item recommendation," *Knowl.-Based Syst.*, vol. 122, pp. 17–25, Apr. 2017.

[51] M. Ghavipour and M. R. Meybodi, "Trust propagation algorithm based on learning automata for inferring local trust in online social networks," *Knowl.-Based Syst.*, vol. 143, pp. 307–316, Mar. 2018.

[52] H. Parvin, P. Moradi, and S. Esmaeili, "TCFACO: Trust-aware collaborative filtering method based on ant colony optimization," *Expert Syst. Appl.*, vol. 118, pp. 152–168, Mar. 2019.

[53] L. Jiang, Y. Cheng, L. Yang, J. Li, H. Yan, and X. Wang, "A trust-based collaborative filtering algorithm for e-commerce recommendation system," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 8, pp. 3023–3034, 2019.

[54] Y. Ruan, P. Zhang, L. Alfantoukh, and A. Durresi, "Measurement theory-based trust management framework for online social communities," *ACM Trans. Internet Techn.*, vol. 17, no. 2, pp. 16:1–16:24, 2017.

[55] S. Adali, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, W. A. Wallace, and G. Williams, "Measuring behavioral trust in social networks," in *Proc. IEEE Int. Conf. Intell. Secur. Informat.*, May 2010, pp. 150–152.

[56] O. Sacco and J. G. Breslin, "In users we trust: Towards social user interactions based trust assertions for the social semantic Web," *Social Netw. Anal. Mining*, vol. 4, no. 1, pp. 1–15, Dec. 2014.

[57] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social trust in opportunistic networks," in *Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops*, Mar. 2010, pp. 1–6.

[58] S. M. Ghafari, S. Yakhchi, A. Beheshti, and M. Orgun, "SETTRUST: Social exchange theory based context-aware trust prediction in online social networks," in *Proc. Int. Workshop Data Quality Trust Big Data, UAE*, 2018, pp. 46–61.

[59] Z. Bo, Z. Huan, L. Meizi, Z. Qin, and H. Jifeng, "Trust traversal: A trust link detection scheme in social network," *Comput. Netw.*, vol. 120, pp. 105–125, Jun. 2017.

[60] N. Ma, E.-P. Lim, V.-A. Nguyen, A. Sun, and H. Liu, "Trust relationship prediction using online product review data," in *Proc. 1st ACM Int. Workshop Complex Netw. Meet Inf. Knowl. Manage. CNIKM*, 2009, pp. 47–54.

[61] Y. Matsuo and H. Yamamoto, "Community gravity: Measuring bidirectional effects by trust and rating on online social networks," in *Proc. 18th Int. Conf. World Wide Web WWW*, 2009, pp. 751–760.

[62] M. Graña, J. D. Nuñez-Gonzalez, L. Ozaeta, and A. Kamińska-Chuchmała, "Experiments of trust prediction in social networks by artificial neural networks," *Cybern. Syst.*, vol. 46, nos. 1–2, pp. 19–34, Feb. 2015.

[63] X. Wang, Y. Wang, and H. Sun, "Exploring the combination of dempster-shafer theory and neural network for predicting trust and distrust," *Comput. Intell. Neurosci.*, vol. 2016, pp. 1–12, Jan. 2016.

[64] K. Zhao and L. Pan, "A machine learning based trust evaluation framework for online social networks," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 69–74.

[65] S. M. Ghafari, A. Joshi, A. Beheshti, C. Paris, S. Yakhchi, and M. Orgun, "DCAT: A deep context-aware trust prediction approach for online social networks," in *Proc. 17th Int. Conf. Adv. Mobile Comput. Multimedia*, Dec. 2019, pp. 20–27.

[66] G. Bachi, M. Coscia, A. Monreale, and F. Giannotti, "Classifying trust/distrust relationships in online social networks," in *Proc. Int. Conf. Privacy, Secur., Risk Trust Int. Conf. Social Comput.*, Sep. 2012, pp. 552–557.

[67] V. Arnaboldi, M. Conti, M. La Gala, A. Passarella, and F. Pezzoni, "Ego network structure in online social networks and its impact on information diffusion," *Comput. Commun.*, vol. 76, pp. 26–41, Feb. 2016.

[68] N. Korovaiko and A. Thomo, "Trust prediction from user-item ratings," *Social Netw. Anal. Mining*, vol. 3, no. 3, pp. 749–759, Sep. 2013.

[69] P. Borzymek and M. Sydow, "Trust and distrust prediction in social network with combined graphical and review-based attributes," in *Proc. KES Int. Symp. Agent Multi-Agent Syst., Technol. Appl.*, Berlin, Germany, 2010, pp. 122–131.

[70] J. Lopez and S. Maag, "Towards a generic trust management framework using a machine-learning-based trust model," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 1343–1348.

[71] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.

[72] K. Zolfaghar and A. Aghaie, "Evolution of trust networks in social Web applications using supervised learning," *Procedia Comput. Sci.*, vol. 3, pp. 833–839, Jan. 2011.

[73] E. D. Raj and L. D. D. Babu, "An enhanced trust prediction strategy for online social networks using probabilistic reputation features," *Neurocomputing*, vol. 219, pp. 412–421, Jan. 2017.

[74] L. Zhao, T. Hua, C.-T. Lu, and I.-R. Chen, "A topic-focused trust model for Twitter," *Comput. Commun.*, vol. 76, pp. 1–11, Feb. 2016.

[75] X. Zhang, L. Cui, and Y. Wang, "CommTrust: Computing multi-dimensional trust by mining E-Commerce feedback comments," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 7, pp. 1631–1643, Jul. 2014.

[76] S. Chakraverty, A. Yadav, and R. Sibal, "On evaluating the effectiveness of rating similarity-based trust," *Social Netw. Anal. Mining*, vol. 6, no. 1, pp. 1–13, Dec. 2016.

[77] J. David Nuñez-Gonzalez, M. Graña, and B. Apolloni, "Reputation features for trust prediction in social networks," *Neurocomputing*, vol. 166, pp. 1–7, Oct. 2015.

[78] M. K. Denko, T. Sun, and I. Woungang, "Trust management in ubiquitous computing: A Bayesian approach," *Comput. Commun.*, vol. 34, no. 3, pp. 398–406, Mar. 2011.

[79] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Netw. Service Manage.*, vol. 8, no. 2, pp. 79–91, Jun. 2011.

[80] V. Sharma, I. You, R. Kumar, and P. Kim, "Computational offloading for efficient trust management in pervasive online social networks using osmotic computing," *IEEE Access*, vol. 5, pp. 5084–5103, 2017.

[81] Y. Wang, X. Wang, J. Tang, W. Zuo, and G. Cai, "Modeling status theory in trust prediction," in *Proc. 29th AAAI Conf. Artif. Intell.*, 2015, pp. 1875–1881.

[82] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the Web," Dept. Comput., Stanford InfoLab, Stanford, CA, USA, Tech. Rep., 1999.

[83] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proc. 13th Conf. World Wide Web WWW*, 2004, pp. 403–412.

[84] J. Golbeck, "Generating predictive movie recommendations from trust in social networks," in *Proc. Int. Conf. Trust Manage.*, iTrust, Italy, 2006, pp. 93–104.

[85] G. Liu, Y. Liu, A. Liu, Z. Li, K. Zheng, Y. Wang, and X. Zhou, "Context-aware trust network extraction in large-scale trust-oriented social networks," *World Wide Web*, vol. 21, no. 3, pp. 713–738, May 2018.

[86] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, Y.-C. Lu, C.-T. Lu, and J. J. P. Tsai, "CATrust: Context-aware trust management for service-oriented ad hoc networks," *IEEE Trans. Services Comput.*, vol. 11, no. 6, pp. 908–921, Nov. 2018.

[87] P. Moradi and S. Ahmadian, "A reliability-based recommendation method to improve trust-aware recommender systems," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7386–7398, Nov. 2015.

[88] S. Sanadhya and S. Singh, "Trust calculation with ant colony optimization in online social networks," *Procedia Comput. Sci.*, vol. 54, pp. 186–195, Jan. 2015.

[89] S. Fazeli, B. Loni, A. Bellogin, H. Drachsler, and P. Sloep, "Implicit vs. Explicit trust in social matrix factorization," in *Proc. 8th ACM Conf. Recommender Syst. RecSys*, 2014, pp. 317–320.

[90] P. Massa and P. Avesani, "Controversial users demand local trust metrics: An experimental study on epinions.com community," in *Proc. 20th Nat. Conf. Artif. Intell.*, vol. 1, 2005, pp. 121–126.

[91] J. Tang, X. Hu, and H. Liu, "Is distrust the negation of trust?: The value of distrust in social media," in *Proc. 25th ACM Conf. Hypertext Social Media HT*, 2014, pp. 148–157.

[92] H. Zhang, Y. Wang, and X. Zhang, "Transaction similarity-based contextual trust evaluation in E-Commerce and E-Service environments," in *Proc. IEEE Int. Conf. Web Services*, Jul. 2011, pp. 500–507.
[93] K. Matsutani, M. Kumano, M. Kimura, K. Saito, K. Ohara, and H. Motoda, "Combining activity-evaluation information with NMF for trust-link prediction in social media," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Oct. 2015, pp. 2263–2272.
[94] J. Tang, H. Liu, H. Gao, and A. Das Sarmas, "ETrust: Understanding trust evolution in an online world," in *Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining KDD*, 2012, pp. 253–261.
[95] J. Huang, F. Nie, H. Huang, and Y.-C. Tu, "Trust prediction via aggregating heterogeneous social networks," in *Proc. 21st ACM Int. Conf. Inf. Knowl. Manage. CIKM*, 2012, pp. 1774–1778.
[96] S. T. Moturu and H. Liu, "Quantifying the trustworthiness of social media content," *Distrib. Parallel Databases*, vol. 29, no. 3, pp. 239–260, Jun. 2011.
[97] Y. Yao, H. Tong, X. Yan, F. Xu, and J. Lu, "MATRI: A multi-aspect and transitive trust inference model," in *Proc. 22nd Int. Conf. World Wide Web WWW*, 2013, pp. 1467–1476.
[98] J. Huang, F. Nie, H. Huang, Y. Lei, and C. Ding, "Social trust prediction using rank-k matrix recovery," in *Proc. 23rd Int. Joint Conf. Artif. Intell. IJCAI*, 2013, pp. 2647–2653.
[99] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," in *Foundations of Intelligent Systems*, vol. 7661. 2012.
[100] K. Su, B. Xiao, B. Liu, H. Zhang, and Z. Zhang, "TAP: A personalized trust-aware QoS prediction approach for Web service recommendation," *Knowl.-Based Syst.*, vol. 115, pp. 55–65, Jan. 2017.
[101] Y. Ruan, A. Durresi, and L. Alfantoukh, "Using Twitter trust network for stock market analysis," *Knowl.-Based Syst.*, vol. 145, pp. 207–218, Apr. 2018.
[102] M. G. Uddin, M. Zulkernine, and S. I. Ahamed, "CAT: A context-aware trust model for open and dynamic systems," in *Proc. ACM Symp. Appl. Comput. SAC*, 2008, pp. 2024–2029.
[103] G. Liu, Y. Wang, and M. A. Orgun, "Social context-aware trust network discovery in complex contextual social networks," in *Proc. AAAI*, 2012, pp. 101–107.
[104] H. Zhang and Y. Wang, "A novel model for contextual transaction trust computation with fixed storage space in E-commerce and E-service environments," in *Proc. IEEE Int. Conf. Services Comput.*, Jun. 2013, pp. 667–674.
[105] K. Zolfaghar and A. Aghaie, "A syntactical approach for interpersonal trust prediction in social Web applications: Combining contextual and structural data," *Knowl.-Based Syst.*, vol. 26, pp. 93–102, Feb. 2012.
[106] H. Zhang, Y. Wang, and X. Zhang, "A trust vector approach to transaction context-aware trust evaluation in e-commerce and e-service environments," in *Proc. 5th IEEE Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Dec. 2012, pp. 1–8.
[107] H. Zhang, Y. Wang, and X. Zhang, "Efficient contextual transaction trust computation in E-commerce environments," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 318–325.
[108] G. Liu, Y. Wang, M. A. Orgun, X. Zheng, A. Liu, Z. Li, and K. Zheng, "Strong social component-aware trust sub-network extraction in contextual social networks," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2016, pp. 107–114.
[109] G. Liu, Y. Wang, M. A. Orgun, and E.-P. Lim, "Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks," *IEEE Trans. Services Comput.*, vol. 6, no. 2, pp. 152–167, Apr. 2013.
[110] G. Liu, Y. Wang, and D. S. Wong, "Multiple QoT constrained social trust path selection in complex social networks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 624–631.
[111] X. Zheng, Y. Wang, and M. A. Orgun, "Contextual sub-network extraction in contextual social networks," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 119–126.
[112] X. Liu and A. Datta, "Modeling context aware dynamic trust using hidden Markov model," in *Proc. 26th AAAI Conf. Artif. Intell. AAAI*, 2012, pp. 1938–1944.
[113] A. Rettinger, M. Nickles, and V. Tresp, "Statistical relational learning of trust," *Mach. Learn.*, vol. 82, no. 2, pp. 191–209, Feb. 2011.
[114] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in *Proc. IEEE Int. Conf. E-Commerce CEC*, Jun. 2003, pp. 275–284.
[115] M. Rehak, M. Gregor, M. Pechoucek, and J. Bradshaw, "Representing context for multiagent trust modeling," in *Proc. IEEE/WIC/ACM Int. Conf. Intell. Agent Technol.*, Dec. 2006, pp. 737–746.
[116] L. Li and Y. Wang, "Context based trust normalization in service-oriented environments," in *Autonomic and Trusted Computing. ATC*. Beijing, China: Springer, 2010, pp. 122–138.
[117] J. Wu, J. Chang, Q. Cao, and C. Liang, "A trust propagation and collaborative filtering based method for incomplete information in social network group decision making with type-2 linguistic trust," *Comput. Ind. Eng.*, vol. 12, Jan. 2019, Art. no. 853864.
[118] R. S. Burt, Y. Bian, and S. Opper, "More or less guanxi: Trust is 60% network context, 10% individual difference," *Social Netw.*, vol. 54, pp. 12–25, Jul. 2018.
[119] J. Li, C. Chen, H. Chen, and C. Tong, "Towards context-aware social recommendation via individual trust," *Knowl.-Based Syst.*, vol. 127, pp. 58–66, Jul. 2017.
[120] R. Ismail and A. Josang, "The beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, 2002, pp. 2502–2511.
[121] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: Trust and reputation in the context of inaccurate information sources," *Auto. Agents Multi-Agent Syst.*, vol. 12, no. 2, pp. 183–198, Mar. 2006.
[122] J. Zhang and R. Cohen, "Evaluating the trustworthiness of advice about seller agents in e-marketplaces: A personalized approach," *Electron. Commerce Res. Appl.*, vol. 7, no. 3, pp. 330–340, Sep. 2008.
[123] E. ElSalamouny, V. Sassone, and M. Nielsen, "Hmm-based trust model," in *Formal Aspects in Security and Trust, FAST*. Beijing, China: Springer, 2010, pp. 21–35.
[124] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-based secure MANET routing using HMMs," in *Proc. 4th ACM Symp. QoS Secur. Wireless Mobile Netw. Q2SWinet*, 2008, pp. 83–90.
[125] X. Zheng, Y. Wang, and M. A. Orgun, "Modeling the dynamic trust of online service providers using HMM," in *Proc. IEEE 20th Int. Conf. Web Services*, Jun. 2013, pp. 459–466.
[126] Z. Malik, I. Akbar, and A. Bouguettaya, "Web services reputation assessment using a hidden Markov model," in *Proc. Int. Conf. Service-Oriented Comput. (ICSOC)*. Mölle, Sweden: Springer, 2009, pp. 576–591.
[127] G. Cai, R. Lv, J. Tang, and H. Liu, "Temporal dynamics in social trust prediction," *Wuhan Univ. J. Natural Sci.*, vol. 19, no. 5, pp. 369–378, Oct. 2014.
[128] M. Laifa, S. Akrouf, and R. Mammeri, "Forgiveness and trust dynamics on social networks," *Adapt. Behav.*, vol. 26, no. 2, pp. 65–83, Apr. 2018.
[129] X. Liu and A. Datta, "A trust prediction approach capturing agents' dynamic behavior," in *Proc. 22nd Int. Joint Conf. Artif. Intell. (IJCAI)*, 2011, pp. 2147–2152.
[130] G. M. Alarcon, J. B. Lyons, J. C. Christensen, M. A. Bowers, S. L. Klosterman, and A. Capiola, "The role of propensity to trust and the five factor model across the trust process," *J. Res. Personality*, vol. 75, pp. 69–82, Aug. 2018.
[131] S. Rothmann and E. P. Coetzer, "The big five personality dimensions and job performance," *SA J. Ind. Psychol.*, vol. 29, no. 1, pp. 1–26, Oct. 2003.
[132] I. Thielmann and B. E. Hilbig, "The traits one can trust: Dissecting reciprocity and kindness as determinants of trustworthy behavior," *Personality Social Psychol. Bull.*, vol. 41, no. 11, pp. 1523–1536, Nov. 2015.
[133] A. M. Evans and W. Revelle, "Survey and behavioral measurements of interpersonal trust," *J. Res. Personality*, vol. 42, no. 6, pp. 1585–1593, Dec. 2008.
[134] R. T. Sicora, "Personality and trust," Ph.D. dissertation, Dept. Comput., Univ. St. Thomas, Saint Paul, MN, USA, 2014.
[135] J. R. Gerris, M. J. Delsing, and J. H. Oud, "Big-five personality factors and interpersonal trust in established marriages," *Family Sci.*, vol. 26, no. 1, pp. 31–39, 2010.
[136] R. S. Solomon, S. Pykl, A. Das, B. Gamback, and T. Chakraborty, "Understanding the psycho-sociological facets of homophily in social network communities," *IEEE Comput. Intell. Mag.*, vol. 14, no. 2, pp. 28–40, May 2019.
[137] S. H. Schwartz, "An overview of the schwartz theory of basic values," *Online Readings Psychol. Culture*, vol. 2, no. 1, pp. 1–20, Dec. 2012.
[138] A. Beheshti, V. Moraveji-Hashemi, S. Yakhchi, H. R. Motahari-Nezhad, S. M. Ghafari, and J. Yang, "personality2vec: Enabling the analysis of behavioral disorders in social networks," in *Proc. 13th Int. Conf. Web Search Data Mining*, Jan. 2020, pp. 825–828.
[139] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 58, no. 7, pp. 1019–1031, 2007.

[140] R. West, H. S. Paskov, J. Leskovec, and C. Potts, "Diffusion-based recommendation with trust relations on tripartite graphs," *Trans. Assoc. Comput. Linguistics*, no. 8, pp. 297–310, 2014.
[141] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Signed networks in social media," in *Proc. 28th Int. Conf. Human factors Comput. Syst. CHI*, 2010, pp. 136–1370.
[142] S.-M.-R. Beheshti, A. Tabebordbar, B. Benatallah, and R. Nouri, "On automating basic data curation tasks," in *Proc. 26th Int. Conf. World Wide Web Companion WWW Companion*, 2017, pp. 165–169.
[143] A. Beheshti, B. Benatallah, A. Tabebordbar, H. R. Motahari-Nezhad, M. C. Barukh, and R. Nouri, "DataSynapse: A social data curation foundry," *Distrib. Parallel Databases*, vol. 37, no. 3, pp. 351–384, Sep. 2019.
[144] A. Beheshti, B. Benatallah, R. Nouri, V. M. Chhieng, H. Xiong, and X. Zhao, "CoreDB: A data lake service," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Nov. 2017, pp. 2451–2454.
[145] A. Beheshti, B. Benatallah, R. Nouri, and A. Tabebordbar, "CoreKG: A knowledge lake service," *Proc. VLDB Endowment*, vol. 11, no. 12, pp. 1942–1945, Aug. 2018.
[146] S.-M.-R. Beheshti, B. Benatallah, S. Venugopal, S. H. Ryu, H. R. Motahari-Nezhad, and W. Wang, "A systematic review and comparative analysis of cross-document coreference resolution methods and tools," *Computing*, vol. 99, no. 4, pp. 313–349, Apr. 2017.
[147] S.-M.-R. Beheshti, B. Benatallah, and H. R. Motahari-Nezhad, "Scalable graph-based OLAP analytics over process execution data," *Distrib. Parallel Databases*, vol. 34, no. 3, pp. 379–423, Sep. 2016.
[148] A. Tabebordbar, A. Beheshti, and B. Benatallah, "Conceptmap: A conceptual approach for formulating user preferences in large information spaces," in *Proc. Int. Conf. Web Inf. Syst. Eng.*, Hong Kong, 2019, pp. 779–794.
[149] A. Tabebordbar, A. Beheshti, B. Benatallah, and M. C. Barukh, "Adaptive rule adaptation in unstructured and dynamic environments," in *Proc. 20th Int. Conf. Web Inf. Syst. Eng.*, Hong Kong, 2019, pp. 326–340.
[150] S. Beheshti, B. Benatallah, S. Sakr, D. Grigori, H. R. Motahari-Nezhad, M. C. Barukh, A. Gater, and S. H. Ryu, *Process Analytics—Concepts and Techniques for Querying and Analyzing Process Data*. Springer, 2016.
[151] A. Beheshti, B. Benatallah, and H. R. Motahari-Nezhad, "ProcessAtlas: A scalable and extensible platform for business process analytics," *Softw., Pract. Exper.*, vol. 48, no. 4, pp. 842–866, Apr. 2018.
[152] S. Beheshti, B. Benatallah, H. R. Motahari Nezhad, and S. Sakr, "A query language for analyzing business processes execution," in *Proc. 9th Int. Conf. Bus. Process Manage.*, Clermont-Ferrand, France, 2011, pp. 281–297.
[153] A. Beheshti, F. Schiliro, S. Ghodratnama, F. Amouzgar, B. Benatallah, J. Yang, Q. Z. Sheng, F. Casati, and H. R. Motahari-Nezhad, "iProcess: Enabling IoT platforms in data-driven knowledge-intensive processes," in *Business Process Management Forum—BPM*, Sydney, NSW, Australia, 2018, pp. 108–126.
[154] S. Beheshti, H. R. Motahari-Nezhad, and B. Benatallah, "Temporal provenance model (TPM): Model and query language," 2012, *arXiv:1211.5009*. [Online]. Available: https://arxiv.org/abs/1211.5009
[155] S. Beheshti, B. Benatallah, and H. R. Motahari-Nezhad, "Enabling the analysis of cross-cutting aspects in ad-hoc processes," in *Proc. 25th Int. Conf. Adv. Inf. Syst. Eng. Adv. Inf. Syst. Eng. CAiSE*, Valencia, Spain, 2013, pp. 51–67.
[156] J. Howe, "The rise of crowdsourcing," *Wired Mag.*, vol. 14, no. 6, pp. 1–4, Jun. 2006.
[157] A. Beheshti, K. Vaghani, B. Benatallah, and A. Tabebordbar, "Crowdcorrect: A curation pipeline for social data cleansing and curation," in *Information Systems in the Big Data Era—CAiSE Forum*, Tallinn, Estonia, 2018, pp. 24–38.
[158] M. Allahbakhsh, A. Ignjatovic, B. Benatallah, S.-M.-R. Beheshti, E. Bertino, and N. Foo, "Reputation management in crowdsourcing systems," in *Proc. 8th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, 2012, pp. 664–671.

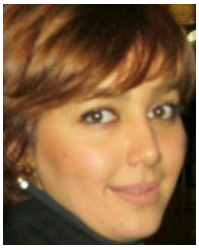
SEYED MOHSSEN GHAFARI received the bachelor's and master's degrees (Hons.) in computer software engineering and the Ph.D. degree from Macquarie University, Sydney, NSW, Australia. He is currently a Data Scientist with industrial companies. His research interest includes data analysis, especially in online social networks.

AMIN BEHESHTI is currently the Director of the AI-Enabled Processes Research Centre and the Head of the Data Analytics Research Laboratory, Department of Computing, Macquarie University. He is also a Senior Lecturer in data science with Macquarie University and an Adjunct Academic in computer science with UNSW Sydney.

ADITYA JOSHI received the Ph.D. degree from the Indian Institute of Technology Bombay, India, and the Ph.D. degree from Monash University, Australia. He is currently a Postdoctoral Fellow with CSIRO Data61. His research interests include natural language processing and machine learning.

CECILE PARIS is currently a Chief Scientist with Data61 and a Group Leader with the Knowledge Discovery and Management, Decision Sciences Research Program, CSIRO Data61. Her research interests include natural language processing and user modeling.

ADNAN MAHMOOD is currently associated with the Department of Computing, Macquarie University, Sydney, NSW, Australia. Before moving to Macquarie University, he spent a considerable number of years in the diverse academic and industrial settings of the Ireland (where he carried research on a project funded and co-funded by Science Foundation Ireland and European Regional Development Fund - Grant Number: 13/RC/2077, respectively), South Korea, Malaysia, Pakistan, and People's Republic of China. His research interests include software-defined networks, network functions virtualization, intelligent transportation systems, the Internet-of-Vehicles, trust management, and next generation heterogeneous wireless networks. He also serves on the technical program committees and editorial boards of several reputed international conferences and journals, respectively.



SHAHPAR YAKHCHI received the bachelor's and master's degrees (Hons.) in computer software engineering. She is currently pursuing the Ph.D. degree with Macquarie University, Sydney, NSW, Australia. Her research interests include data analysis and recommender systems.

MEHMET A. ORGUN (Senior Member, IEEE) is currently a Professor with the Division of Information and Communication Sciences, Department of Computing, Macquarie University, Sydney, NSW, Australia. His current research interests include computational intelligence, multiagent systems, trust and security, temporal reasoning, and formal methods.