Sharing Reputation Data Across Online Communities

Mohammad Allahbakhsh and Haleh Amintoosi, *Ferdowsi University of Mashhad, Mashhad, 1696700, Iran*
Schahram Dustdar, *TU Wien, 1040, Vienna, Austria*
Hamid-Reza Motahari-Nezhad, *Macquarie University, Sydney, N.S.W., 2109, Australia*

Today, people are often members of several online communities, leaving their footprints scattered across cyberspace in the form of local reputations. Collecting these reputation data to build a global reputation becomes increasingly necessary. This article proposes a new perspective on the topic of sharing reputation data across online communities. We discuss the notion of global reputation, propose a taxonomy for reputation data sharing and use it to briefly study the related literature, and identify and discuss some of the key challenges towards reputation data sharing. To encourage future research, we also propose a conceptual model for global personalized reputation management.

Trust and reputation are cornerstones of all online transactions and interactions between parties in online communities.[1] An online interaction, for example, an online purchase, occurs when the buyer, to some extent, mutually trusts the seller. For cases in which two parties have no prior relationships, their reputation scores are used as a proxy and the judgment of the community on their trustworthiness. The reputation score of a community member is an aggregation of the feedback received from other members on their experience interacting with him/her alongside other personal or community-focused information items.[2] Due to their impact on the popularity, gains, monetary and nonmonetary benefits of the members, several research works show that reputation systems are often subject to attacks.[1] A large body of research is devoted to proposing fair reputation computational models in existing human-enabled platforms. Examples are fuzzy,[3] Bayesian, belief theory, and analytical models (e.g., weighted sum, iterative techniques).[2]

1089-7801 © 2022 IEEE
Digital Object Identifier 10.1109/MIC.2022.3155065
Date of publication 28 February 2022; date of current version 19 July 2022.

A typical person is often a member of more than one platform where he/she has a profile and a history upon which a reputation is built. In other words, reputation scores scattered across multiple platforms are collectively referred to as social credentials.[4]

Under several data and privacy policies, members own their data, and it is their right to be able to share these credentials across platforms. This sharing is crucial since it prevents problems such as members' loss of income and personal/social opportunities, and platform lock-in. Several research articles, as well as start-ups and platforms, have been proposed to study this problem from various points of view such as cross-organizational interactions,[5] privacy preservation,[6] portability of reputation,[4] and client–server interactions.[7] However, there is still no easy practical way for sharing reputation data. This is because of challenges such as reluctance of platforms, legal challenges, privacy considerations, and technical and interoperability issues.

Despite these challenges, demand from the users' side to have their social credentials collected and be aware of what data items platforms collect about them is ever-increasing.[8] Moreover, the interest and commitment of governments towards forcing public and private sectors, thorough legislation and policy making, to honor data ownership and portability are growing. In other words, these pro-user

legislations, such as regulations established in the California state government,[a] the European Union,[b] or China,[c] states that users own their data and should be able to take and move it across platforms, and the platforms should facilitate this. These legislative obligations besides community demand will act as a serious driving force towards reputation sharing in the future.

On the other hand, organizations of tomorrow are likely to be open and decentralized and will rely on distributed power sharing control structures through network protocols and peer-to-peer transactions. Arcade City (https://arcade.city/), a fully distributed ride-sharing app, is an example of such organizations that are run by its member drivers, and all its revenue is shared among them. There are other examples of decentralized organizations such as Dash[d] and PolkaDAO[e] each with its own version of decentralized structure and network protocols. This shift in the structure of the organizations makes reputation sharing a more challenging topic to study.

Analyzing and addressing the problem of sharing reputation data needs a fundamental understanding of all involved entities and factors, challenges and opportunities, and a conceptual model that brings all these aspects under one umbrella.

ESTABLISHING AND SHARING REPUTATION

Global Reputation

The trustworthiness of a community member can be studied at three levels. The first and the lowest level is the pairwise trust among members, which is computed directly based on their mutual interactions.

The second level is community-wide trustworthiness, where every member has one local reputation score, which is the community-wide judgment of his/her trustworthiness. There is a plethora of research to compute reputation scores.[9]

The third level is global reputation, defined as follows:

> The global reputation of a person is the overall judgment of his/her trustworthiness across cyberspace.

Global reputation is an aggregation/combination of the local reputation scores and/or other reputation-related data that comes from different platforms. Each of the community-wide reputation scores may reflect a specific aspect of the member's profile. Combining these scores to build a single value as global reputation may not be neither reasonable nor feasible. Consequently, we view global reputation as a multidimensional data structure that reflects different aspects of the member's trustworthiness. Aggregating these reputation scores, when coming from the same context and having the same trust computation and data models is feasible.[10] However, it is not the case in general. There is no widely adopted approach or platform for global reputation computation. These challenges are discussed in more detail in "Towards a Global Personalized Reputation Sharing Model" section.

Reputation Sharing Taxonomy

Sharing the reputation data is a process in which, four main entities are involved: two engaging communities, the shared data, and possibly a third-party mediator. Online communities, called sharing parties A and B (as illustrated in Figure 1), share data, referred to as shared reputation data. The data may be shared directly or through a mediator, which moderates the reputation-sharing process. The data sharing is governed by global (inter-platform) and local (intra-platform) regulations and policies. Reputation sharing is characterized along four main dimensions, i.e., *shared data*, *sharing method*, *sharing granularity, and sharing directions*.

Shared Data

Data can be shared in three different forms. The most common form is *aggregated reputation data* that represents the members' local reputation in forms of scores, stars, badges, and plugins.[11] In this form, the receiving party has no idea about the raw data and the aggregation techniques, and only receives an opaque score that comes from an outside source, i.e., the provider party.

Sharing *raw data*, as another form, means that the system shares the raw, nonaggregated data with other communities.[10] In this form, the receiving party may take the data, apply his own techniques, and create system-dependent reputation scores.

In some systems, the reputation of the user depends on his/her *identification data.* For instance, on Twitter, a blue star next to the name of the member implies that his/her identity has been verified. In such

[a][Online]. Available: https://oag.ca.gov/privacy/ccpa
[b][Online]. Available: https://gdpr.eu/
[c][Online]. Available: https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/
[d][Online]. Available: https://www.dash.org/
[e][Online]. Available: https://polkadot.network/about

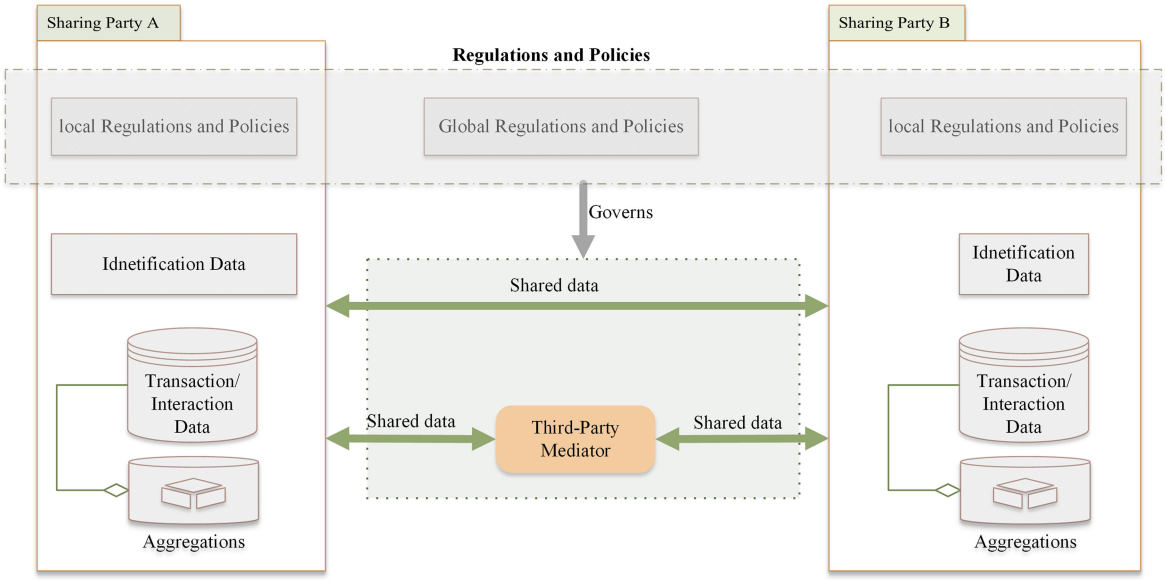

FIGURE 1. Reputation Sharing Process.

a case, this identity can be shared via e.g., Open Authentication services,[f] to verify the member's identity in other communities.[12]

Sharing Method

Data may be shared in three methods. In the *centralized* method, all sharing parties send their shared data to a single third-party mediator, which collects and shares information amongst the parties.[11] The mediator either shares raw data, aggregated data or knowledge extracted from the data.

In the *P2P* method, a pair of parties share their information[12] and compute partial global reputation scores. These pairwise scores are based on the information collected only from these two parties, and hence, are different from pair to pair.

In a *decentralized* method, more than one mediator/coordinator monitors and approves the trustworthiness of parties.[1] Consensus mechanisms used in Blockchain-based trust management systems are examples of decentralized data sharing.[13]

Centralized methods are simple and easy to implement and manage for data exchange and conversion. However, the central coordinator can become a single point of failure. P2P methods facilitate the interactions without needing a centralized coordinator. On the downside, they would compute a partial reputation score rather than a global one. They are also prone to collusion between malicious pairs. Decentralized systems are more complex from implementation and update propagation points of view. On the upside, they enable a higher level of availability compared to the centralized methods. They are also more robust to reputation attacks compared to P2P methods.

Sharing Granularity

The data sharing may happen at two granular scales. At the *member scale*, the history or reputation data of a single or a subset of members is shared. For instance, in the past, Amazon allowed users to import their ratings from eBay.[10] In such a scenario, due to partial sharing of information, the computed reputation scores are less dependable and prone to collusion.

At the *system scale*, all information of a system is shared or at least is available for sharing. In such a case, the computed reputation scores are more reliable. However, in the real world, platforms are reluctant to share their information and they would prefer member scale, if at all.[14] This level of information sharing is more common for the systems that are owned or managed under the same administration. Sharing information between YouTube, Gmail, and other Google services is an example of such a system scale information sharing. This experience of successful information sharing is evidence justifying that if the technical and business barriers are handled, members can benefit from sharing their reputation across various platforms.

[f][Online]. Available: https://openauthentication.org/

Sharing Direction

Reputation data can be shared between sharing parties, either unidirectional or bidirectional. In unidirectional mode, sharing parties may either act as data providers or data consumers.[4] Consumers take advantage of data collected from providers and do not share back any information with them.

In *bidirectional* mode, sharing parties act both as providers and consumers, and share computed reputation.[7]

REPUTATION SHARING IN PRACTICE

The idea of reputation data sharing dates back to the early stages of Web 2.0 when people started using online platforms such as eBay and Amazon.[10] Investigating different aspects and challenges of reputation sharing has always been a serious concern. Hesse and Teubner,[15] empirically have conducted a consumer survey on perceptions of reputation portability. Platforms' reluctance to share data is discussed in the article by Teubner *et al.*[10] Fan *et al.*[1] have reviewed different designs of decentralized trust management models and compared their robustness against threats. They also provide three design principles for decentralized trust management. Teubner *et al.*[16] studied the cross-platform reputation transfer challenge and discussed future research opportunities such as data ownership and legal considerations, boundary conditions of reputation transfer, and user interface design.

Several *research prototypes* are proposed for solving the reputation sharing problem. In Gal-Oz *et al.*,[11] a three-stage reputation sharing model is proposed that assumes the willingness of platforms to share data, which is not often the case.

Hesse and Teubner[4] investigate reputation transferability as an aspect of digital identity management and then present a conceptual model demonstrating the important mechanisms and actors. A centralized interoperable privacy-preserving reputation system is introduced in the article by Pingel and Steinbrecher.[6]

Inspired by how reputation is transferred in illegal drug markets, Norbutas *et al.*[17] proposed a reputation sharing model to transfer the reputation history from a stopped market to a new one. Using cryptographic schemes, sellers can migrate their identity and reputation to the new market anonymously.

In CloudArmor,[12] authors propose collusion-aware and attack-resilient techniques for trust management in cloud services. Skopik *et al.*[5] propose a centralized reputation management model based on the social notion of trust, in cross-organizational interactions.

In addition to research prototypes, there are also some efforts to create **reputation-sharing platforms**. Deemly (deemly.co), Traity (traity.com), TrustCloud (trustcloud.com), and WhyTrusted (whytrusted.com) are among such efforts.[16,18]

Deemly enabled users to collect reputation ratings from P2P markets. Traity presented the reputation passport concept and offered reputation ownership to its members. TrustCloud provided its users with a portable reputation score to facilitate their involvement in online transactions. WhyTrusted aimed at aggregating the reputation data of its users and tracking their online reputation trial. These platforms have not been successful, as they had not considered trust, privacy, business, and data availability challenges. To the best of our knowledge, Truste, recently named TrustArc (trustarc.com), is the only active platform. However, its focus is on the privacy aspect of reputation sharing.

A general challenge ahead of reputation-sharing platforms is that users need to share their personal access credentials with platforms to enable them to collect their reputation data. This requires a high level of trust in the platform, which turned into the Achilles heel for their success and resulted in the failure of almost all reputation-sharing initiatives.

Looking at both the research literature and platforms reveals that existing attempts focus more on technical and interoperability aspects of reputation sharing, and pay less attention to personal, social, and legal aspects. This is the main problem that we discuss and aim to address by proposing a personalized context-aware conceptual global reputation model. A summary of the related literature studied based on our proposed taxonomy, is presented in Table 1.

OPEN CHALLENGES

Global reputation sharing faces several challenges that need to be investigated, some of which fall out of the scope of this research, such as software engineering challenges. Here, we focus only on the most important challenges, in our view, that directly affect the success of reputation sharing.

Rights, Ownership, and Regulations

In addition to the content directly generated by users, there are data items that are collected or generated based on their behavior. Likes, dislikes, post views, connections, and other interactions between the user

TABLE 1. Summary of the Related Works.

#	Related Work	Shared Data	Method	Granularity	Direction
1	[11]	Aggregated Data	Centralized	Member	Bidirectional
2	[6]	Raw Data	Centralized	Member	Bidirectional
3	[17]	Raw and Aggregated Data	Centralized	Member	Bidirectional
4	[12]	Raw and Identification Data	P2P	Member	Bidirectional
5	[5]	Raw and Aggregated Data	Decentralized	Member	Bidirectional
6	[7]	Aggregated Data	Decentralized	Member	Bidirectional
7	[4]	Aggregated Data	Centralized	Member	Unidirectional
8	Deemly (deemly.co)	Aggregated Data	P2P	Member	Bidirectional
9	Traity (Traity.com)	Aggregated Data	Centralized	Member	Bidirectional
10	TrustCloud (TrustCloud.com)	Raw and Aggregated Data	Centralized	Member	Bidirectional
11	Whytrusted (whytrusted.com)	Aggregated Data	P2P	Member	Bidirectional

and the community/platform are examples of the user behaviors upon which the reputation of users, quality of posts, and many more forms of analytics rely. The ownership and copyright of these data items have sparked challenging debates. For instance, when Amazon allowed its users to import their ratings from eBay, eBay stopped it by claiming the ownership of data.[10] Recently, the European Union has tried to solve it by passing legislation related to data protection (GDPR). This inspired China, Brazil, Canada, and the California state government to pass or consider passing similar legislation. Although these rules do not clarify the ownership of data, they give the user the right to have access to that information, ask them to be erased, object their sale, and importantly receive them "in a machine-readable format and send it to another controller." The latter, which they call data portability, can be used as a basis for sharing reputation data. The case where data items have more than one involved member with conflicting sharing interests is still a challenge that needs to be addressed.

Collecting and aggregating reputation-related information of a member from all around cyberspace creates serious concerns. No matter who owns the platform, whether the government or the private sector, there is always the possibility of the information being misused for commercial or political purposes. However, there are justifications for taking such a risk. The first is the necessity/benefits of reputation sharing. The second is that there are regulations, established or highly demanded, for preventing authorities' access to certain types of information without judicial permissions. Third, and from the technical point of view, decentralized and member-owned data sharing models can provide another interesting direction for handling such a risk.

Data Credibility

The credibility level of the data collected from various communities is another challenge. To compute reliable global reputation scores, the credibility of the shared data should be considered during data aggregation. Data coming from credible/authorized parties should have a bigger footprint in reputation score than the one from less credible sources. Who should be in charge of defining and assessing these credibility levels? How should the global reputation computation system handle the possible misinformation or disinformation? These are just examples of challenging questions to be answered.

Business Competition

Data collected from members is the main asset of platforms that are active in different domains and contexts. On one hand, sharing data between platforms from different contexts is neither useful nor simply feasible. On the other hand, the communities that have similar contexts are naturally business competitors, and sharing reputation can boost their competitors and probably negatively affect their revenue. Consequently, they have the least incentives to share their data. The main challenge here is a tradeoff between the benefits of sharing data and the consequences of sharing data with a competitor.

Privacy Preservation

Sharing users' data among communities with or without users' consent can raise serious privacy challenges.

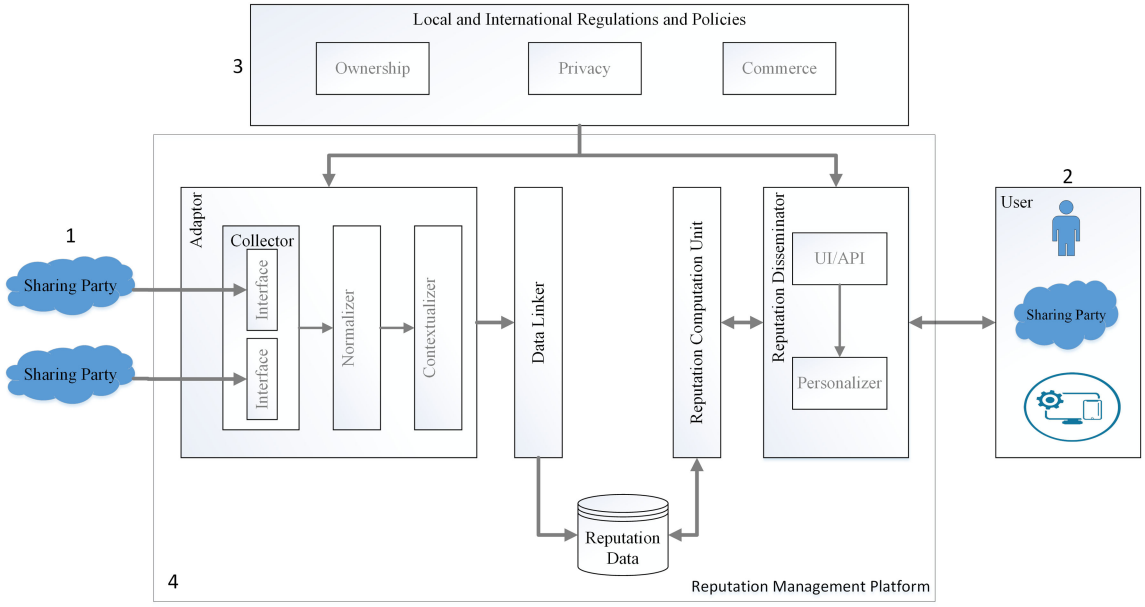

FIGURE 2. Conceptual model for reputation sharing.

In an ordinary situation, users' information is scattered across cyberspace, and it is unlikely to breach their privacy. Collecting members' information in one platform may lead to data accumulation, and increase the risk of a privacy breach.

Interoperability

Different communities may use different technologies for saving or representing content and data. To be able to share data, parties should follow specific interoperability standards, protocols, and guidelines, regardless of their internal technologies. These standards should provide general guidelines for sharing different data types. Currently, there is a lack of such standards or guidelines. Establishing such standards is challenging due to the heterogeneity of the platforms and their internal technologies. Being widely accepted and used by the communities is another challenge regarding the design of such guidelines.

Technical Difficulties

Last but not the least, sharing reputation data across online communities is technically challenging. Lack of expertise and technical skills, inefficient platform design, and security vulnerabilities can pump many noncredible data into other communities, hence directly affecting the credibility of computed reputation scores.

Different sharing parties may use different trust computational models, data models, and architectures. Hence, aggregating reputation data is a technical challenge. Defining conversion interfaces between sharing parties can partially address this challenge.[11] However, adopting the changes made in two sharing parties may necessitate updating or changing the sharing interfaces between communities, which is a technical overhead.

TOWARDS A GLOBAL PERSONALIZED REPUTATION SHARING MODEL

In light of the previously mentioned challenges in existing prototypes and platforms, we proposed a conceptual model for sharing reputation data. In the proposed model, as shown in Figure 2, there exist four main components:

1) Sharing parties that act as reputation data providers.
2) Users (a sharing party, a software application, or a human user) who consume the computed reputation information.
3) Local and international regulations and policies.
4) Reputation management platform.

The reputation management platform comprises four components.

The *Adapter* is responsible for collecting reputation data. Data is collected through interfaces specifically designed for each sharing party. These interfaces control the data import according to the local and international regulations, contextual information, and obligations of both data provider and reputation management platform. Since the collected data comes from various sources with different ranges, standards, and representations, they should be normalized to be aggregable with data collected from other parties. This is done by the normalizer. Moreover, the collected data may come from various contexts. The reputation management system may have a database of some predefined contexts, and information on how to compare and convert contexts, and what aspects of a member's profile are covered by each of these contexts. The contexts are defined in standard formats, and the contextualizer is responsible for converting normalized data to these formats.

The normalized contextualized data is then passed to the *data linker*, which builds up a general profile for each member by linking his/her reputation data collected from various providers. The linker needs to identify members correctly and uniquely in each data provider to link their data correctly. These general profiles are then stored in a database.

Our conceptual model aims to compute personalized reputation scores. More precisely, the computed reputation score depends on the profile of the user who queries the reputation information, the members whose reputation scores are being queried, and possible local and international regulations and policies.

Users can utilize the *reputation disseminator* to query the reputation of a member through a UI or an API. Disseminator collects all required information and passes them to the *reputation computation unit*. This unit computes a personalized contextualized reputation score for the member and sends it back to the disseminator to be delivered to the user.

It is notable that the implementation of this model is application-dependent. It can be centralized, decentralized, or hybrid with some components centralized and others decentralized.

As we move towards DAOs,[g] the impact of social and legal factors becomes more important, being partially or fully ignored in existing platforms. The decentralized implementation of our model may become efficient and desirable in such scenarios.

CONCLUSION

While desirable by members to own and transfer their reputation data across different platforms, the reputation-sharing practices have not been effectively successful so far due to challenges such as platform reluctance, legal challenges, privacy considerations, and technical issues, Government and public legal frameworks have been advocating users by forcing public and private sectors to honor data ownership and portability. With the acceleration of Blockchain-based technology in every aspect of our life, organizations are also moving towards distributed and autonomous architectures. All these trends and advances suggest that reputation sharing will become more desirable and potentially reachable in the form of peer-to-peer reputation data-sharing models, sharing consortiums, or decentralized reputation sharing platforms. Besides technical considerations, paying attention to personal, legal, and social aspects of data sharing will be a key success factor in every reputation data-sharing attempt.

The taxonomy proposed in this research helps gain a better understanding of different aspects of the reputation-sharing problem. We also propose a conceptual model for sharing reputation data to provide some basic guidelines for developing reputation-sharing platforms.

REFERENCES

1. X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, "Decentralized trust management: Risk analysis and trust aggregation," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–33, 2020.
2. A. Jùsang, 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, 2007.
3. M. Allahbakhsh, H. Amintoosi, A. Ignjatovic, and E. Bertino, "A trust-based experience-aware framework for integrating fuzzy recommendations," *IEEE Trans. Serv. Comput.*, vol. 15, no. 2, pp. 698–709, Mar./Apr. 2022, doi: 10.1109/TSC.2019.2956937.
4. M. Hesse and T. Teubner, "Reputation portability–quo vadis?," *Electron. Markets*, vol. 30, pp. 331–349, 2019.
5. F. Skopik, D. Schall, and S. Dustdar, "Modeling and mining of dynamic trust in complex service-oriented systems," in *Socially Enhanced Services Computing: Modern Models and Algorithms for Distributed Systems*. Vienna, Austria: Springer, 2011, pp. 29–75.
6. F. Pingel and S. Steinbrecher, "Multilateral secure cross-community reputation systems for internet communities," in *Proc. Int. Conf. Trust, Privacy Secur. Digit. Bus.*, 2008, pp. 69–78.

[g]Decentralized Autonomous Organization

7. A. Basu, I. Wakeman, D. Chalmers, and J. Robinson, "A behavioural model for client reputation," in *Proc. Trust Mobile Environ.*, 2008, pp. 1–13.
8. J. Isaak and M. J. Hanna, "User data privacy: Facebook, Cambridge Analytica, and privacy protection," *Computer,* vol. 51, no. 8, pp. 56–59, 2018.
9. J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Comput. Commun.,* vol. 97, pp. 1–14, 2017.
10. T. Teubner, M. T. Adam, and F. Hawlitschek, "Unlocking online reputation," *Bus. Inf. Syst. Eng.*, vol. 62, pp. 501–513, 2019.
11. N. Gal-Oz, T. Grinshpoun, and E. Gudes, "Sharing reputation across virtual communities," *J. Theor. Appl. Electron. Commerce Res.,* vol. 5, no. 2, pp. 1–25, 2010.
12. T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.
13. Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–28, 2021.
14. M. Kokkodis and P. G. Ipeirotis, "Reputation transferability in online labor markets," *Manage. Sci.*, vol. 62, no. 6, pp. 1687–1706, 2016.
15. M. Hesse and T. Teubner, "Takeaway trust: A market data perspectiveon reputation portability in electronic commerce," in *Proc. 53rd Hawaii Int. Conf. Syst. Sci.*, 2020, pp. 5119–5128.
16. T. Teubner, F. Hawlitschek, and M. T. Adam, "Reputation transfer," *Bus. Inf. Syst. Eng.,* vol. 61, no. 2, pp. 229–235, 2019.
17. L. Norbutas, S. Ruiter, and R. Corten, "Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets," *Int. J. Drug Policy*, vol. 76, 2020, Art. no. 102635.
18. J. Zhang, "Trust transfer in the sharing Economy—A survey-based approach," *Junior Manage. Sci.*, vol. 3, no. 2, pp. 1–32, 2018.

MOHAMMAD ALLAHBAKHSH is currently an associate professor with the Ferdowsi University of Mashhad, Mashhad, 1696700, Iran. His main research interests include quality control and data aggregation in human-enabled applications, decentralized systems, and augmented intelligence. Allahbakhsh received his Ph.D. degree in computer science and engineering from The University of New South Wales, Sydney, NSW, Australia. Contact him at allahbakhsh@um.ac.ir.

HALEH AMINTOOSI is an assistant professor with the Ferdowsi University of Mashhad, Mashhad, 1696700, Iran. She is also a Visiting Senior Lecturer with the School of Computer Science and Engineering, The University of New South Wales (UNSW), Sydney, NSW, Australia. Her main research interests include trust and privacy in crowdsourcing and crowdsensing systems, authentication protocols, and blockchain. Amintoosi received her Ph.D. degree in computer science and engineering from UNSW. Contact her at amintoosi@um.ac.ir.

SCHAHRAM DUSTDAR is full professor of computer science heading the Research Division of Distributed Systems at the TU Wien, 1040, Vienna, Austria. In 2021, he was elected to the Academy of the United Nations Sciences and Technology Organization (AUNSTO). He is an elected member of the Academia Europaea: The Europe, where he is the chairman of the Informatics Section, as well as an IEEE fellow. Contact him at dustdar@dsg.tuwien.ac.at.

HAMID-REZA MOTAHARI-NEZHAD is a visiting professor of computer science with the Department of Computing, Macquarie University, Macquarie Park, NSW, 2109, Australia, with a research interest in artificial intelligence, human-AI interaction models, and distributed blockchain-based systems. He is a senior member of IEEE. Contact him at hamidreza.motaharinezhad@mq.edu.au.