IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 11, 2018, accepted January 16, 2019, date of publication January 23, 2019, date of current version March 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2894344

Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services: From Multiple Perspectives

KE YAN[1], (Member, IEEE), WEN SHEN[2], QUN JIN[1,3], (Senior Member, IEEE), AND HUIJUAN LU[1]

[1]College of Information Engineering, China Jiliang University, Hangzhou 310018, China
[2]Department of Informatics, University of California at Irvine, Irvine, CA 92697, USA
[3]Department of Human Informatics and Cognitive Sciences, Waseda University, Tokorozawa 359-1192, Japan

Corresponding author: Qun Jin (jin@waseda.jp)

This work was supported in part by the National Natural Science Foundation of China under Grant 61850410531, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY19F020016, and in part by the National Natural Science Foundation of China under Grant 61602431.

ABSTRACT Fast development of shared services has become a crucial part of the cyber-enabled world construction process, as sharing services reinvent how people exchange and obtain goods or services. However, privacy leakage or disclosure remains a key concern during the sharing service development process. While significant efforts have been undertaken to address various privacy issues in recent years, there is a surprising lack of review for privacy concerns in the cyber-enabled sharing world. To bridge the gap, in this paper, we survey and evaluate existing and emerging privacy issues relating to sharing services from various perspectives. Differing from existing similar works on surveying sharing practices in various fields, our work comprehensively covers six branches of sharing services in the cyber-enabled world and selects solutions mostly from the recent five to six years. We conclude the issues and solutions from three perspectives, namely, from users', platforms' and service providers' perspectives. Hot topics and less discussed (cold) topics are identified, which provides hints to researchers for their future studies.

INDEX TERMS Cyber technology, sharing service, privacy, crowdsourcing, collaborative consumption.

I. INTRODUCTION

Cyberization is transforming our physical living world into a virtual computerized world by leveraging the Internet and computational methodologies [1], [2]. In the virtual computerized world, or more specifically, the cyber-enabled world, people are connected via Internet regardless of physical distances. Cyber-enabled sharing services, or in short, sharing services, which provide information, goods, and services in a shared form to multiple individuals, who know or do not know each other, are essential and necessary components of cyber-world development and probably the most exciting cyber-related concept in the current stage of cyberization. Sharing services encourage people to share both virtual and physical assets through the Internet using cyber-enabled clients, including mobile phones, all kinds of computers and similar digital devices. Sharing services contribute to the fast development of cyber technology, where the control, responsibility for the common good, earnings, capitalization, information, and efforts are all shared among the participants or distributed to peer members [3]. In recent years, cyberized sharing service companies, such as Uber, Airbnb, Etsy and Amazon Family Library, have been overwhelmingly popular and enjoyed incredible growth [4], [5].

There are various reasons for people to participate in sharing practices. For instance, no single entity or person can control the whole market or economy, although some participants have more regulatory power than others. All participants share the responsibility of making the market to operate healthily. This form of collaborative economy or peer-to-peer (P2P) sharing leads to more efficient resource allocations and more sustainable lifestyles. However, any participant in the sharing practice, regardless whether it is a user or service provider, can be a potential attacker who compromises legitimate users' privacy. Therefore, to attract more people to share, it is necessary to build trust, establish reputation, protect privacy and guarantee security for both the user and

service provider [6]. Personal privacy concern is the main factor that hinders the development of sharing services in the cyber-enabled world [7], [8]. On one hand, people are reluctant to adopt sharing practices due to privacy disclosure concerns [9]–[11]; on the other hand, sharing service providers insist that personal data is part of the necessary information in user experience analysis for improving service quality. While only privacy protection is explored in this paper, the authors would like to note that privacy is relevant and closely related to trust, reputation and security. Users need to trust the service provider, which implies that the service provider must have a good reputation that the users can trust. Reputations are established through the interactions between the users and service providers. However, during the interaction process, privacy issues arise, since private information pieces from both parties are inevitably revealed to each other [12], [13].

Unfortunately, due to the fast development pace of sharing service technology, privacy issues were not well addressed before sharing services were widely spread over the physical world [14]. For example, in the ridesharing service practice, although the business model exists for quite a while, there are still many privacy leakage concerns, including location privacy concerns, driver/customer's personal information leakage concerns, physical privacy concerns and etc. [15]. Cyber-technologies that can be used to protect various aspects of privacy are urgently desired to prohibit both the user and service provider from revealing each other's sensitive information. In the starting stage of the sharing economy, some service providers intentionally neglect the privacy issues to survive in the highly competitive business environment. In other words, profit is usually the highest priority for most starter-level sharing service companies. In this study, we surveyed over one hundred research works from recent years that are closely related to the privacy issues with the newly developed sharing service technologies and observed that the privacy protection level is highly related to the number of users who participate in the sharing service, which affects the final profit of the service providers. In addition, from the user's perspective, increasing the self-awareness of privacy disclosure is an important task for the users to protect themselves in the current stage of cyberization.

In summary, the emerging privacy issues of sharing services in the cyber-enabled world and the available solutions are reviewed comprehensively. From the literature, we summarize the sharing services in the current stage of the cyber-enabled world into two categories [3], [16]:

- **Crowdsourcing** employs collective intelligence or power to fulfil tasks or achieve goals. Concrete examples of crowdsourcing are Internet crowdsourcing marketplaces, crowdfunding, and crowdtesting [17]. For a typical crowdsourcing practice, there are, in general, three roles involved: the task requester, the platform and the worker. The task requester posts tasks on the platform and attracts workers to finish the job in a crowdsourcing way.
- **Collaborative consumption** allows consumers to use products or services without full ownership. Concrete examples of collaborative consumption include collaborative online shopping, ridesharing, and homesharing practices [5]. For a typical collaborative consumption model, there are again three roles involved: the host, the platform and the customer. Differing from the crowdsourcing practice, the host provides P2P sharing of goods or services to customers through an online platform.

In this study, we refer to the combination of task requesters and hosts as service providers, and the combination of workers and customers as users. The review of privacy issues and solutions follows the above two outlines and reveals the main concerns in the literature, which include the requester's data protection, the balance between privacy protection and sacrifice, data encryption, unreliable data analysis, location privacy and physical privacy. Figure 1 lists a taxonomy of important works that are surveyed for privacy issues and solutions in crowdsourcing and collaborative consumption practices.

Although there are similar works concerning privacy in sharing practices from the literature, e.g., [18]–[22], they focused on traditional privacy protection methods. Traditional privacy protection techniques, including k-anonymity [23], [24], l-diversity [25] and t-closeness [26], have been heavily reviewed in the past few decades. In contrast, our work focuses on privacy protection technique development in recent years, skips the traditional approaches and covers technologies comprehensively in the area of cyber-enabled sharing services. Most surveyed works in this study were published in past five to six years. The sources of the reviewed papers include the most popular databases, such as ACM Digital Library, IEEE Xplore Digital Library, Springer Link and ScienceDirect. The searched keywords include 'sharing service', 'privacy issue', 'privacy protection', 'crowdsourcing privacy', 'collaborative consumption privacy', 'crowdfunding privacy' and etc.

The main contributions of this work include 1) categorizing recent research studies working on privacy issues of sharing services into trends, 2) identifying the hot/cold research topics, and 3) finding the research gaps for real-world sharing services to better protect people's privacy. For example, from Fig. 1, we found that data reliability analysis and location privacy are two hot topics for collaborative consumption, whereas the physical privacy issue in homesharing practice is less discussed. Moreover, there are research works indicating that physical privacy is also largely concerned by users in the sharing service practices. Those less discussed topics require more attention in future studies.

The remaining parts of this work are organized as follows: The emerging privacy issues and solutions of crowdsourcing are analyzed in Section II. The emerging privacy issues and solutions of collaborative consumption are reviewed in Section III. In Section IV, all six branches discussed in Sections II and III are summarized from three perspectives,

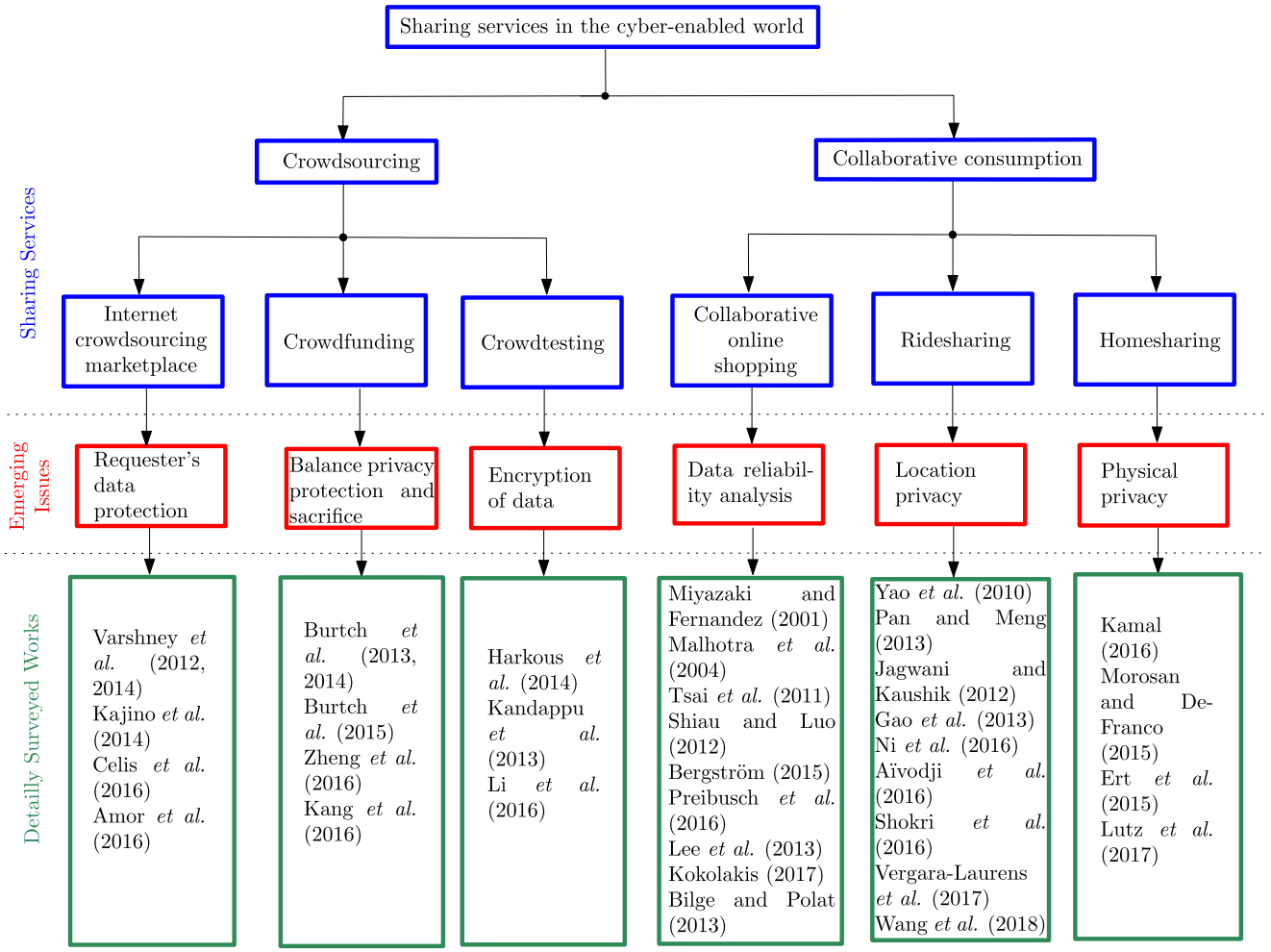

FIGURE 1. Taxonomy of sharing services in the cyber-enabled world following the categorization of crowdsourcing and collaborative consumption practices (in blue rectangles), with identified emerging privacy issues (in red rectangles) and surveyed works in the literature (in green rectangles).

namely, user, platform and service provider perspectives. Section V raises open research issues for each branch of the sharing services and from the three perspectives mentioned in Section IV. In Section VI, several conclusions are drawn regarding cyber technology development to predict the future trends in the development of cyber-enabled sharing technologies.

II. PRIVACY ISSUES AND SOLUTIONS IN CROWDSOURCING PRACTICES

Crowdsourcing refers to the distribution of tasks that cannot be easily accomplished in a traditional way to a large group of online workers [27] (Figure 2). The tasks are usually difficult problems or issues that cannot easily be resolved by small groups of users or individuals. Despite its many advantages, crowdsourcing brings increasing risks of information leakage and privacy violation, which limits its development and application potential.

There are two types of users in a crowdsourcing platform: the worker (or the employee) and the task requester (or the employer). The task requester provides incentives and tasks, while the worker performs the tasks to receive the incentives. The interaction between them gives rise to the risks of information leakage and privacy violation, which is either unidirectional or bidirectional. In other words, either the worker or the requester, or both, have the possibility to leak sensitive information or violate the privacy agreement.

We next identify potential privacy leaking risks in three key applications of crowdsourcing: Internet crowdsourcing marketplaces, crowdfunding, and crowdtesting. For each application, we consider the privacy protection issues in the process of sharing practice and survey the existing solutions in the literature.

A. CROWDSOURCING MARKETPLACE

An online crowdsourcing marketplace provides a platform for matching the task requesters and the task performers for mutual benefits. Numerous crowdsourcing marketplaces have been developed during the past few years, e.g., the Amazon Mechanical Turk (MTurk) [28], which

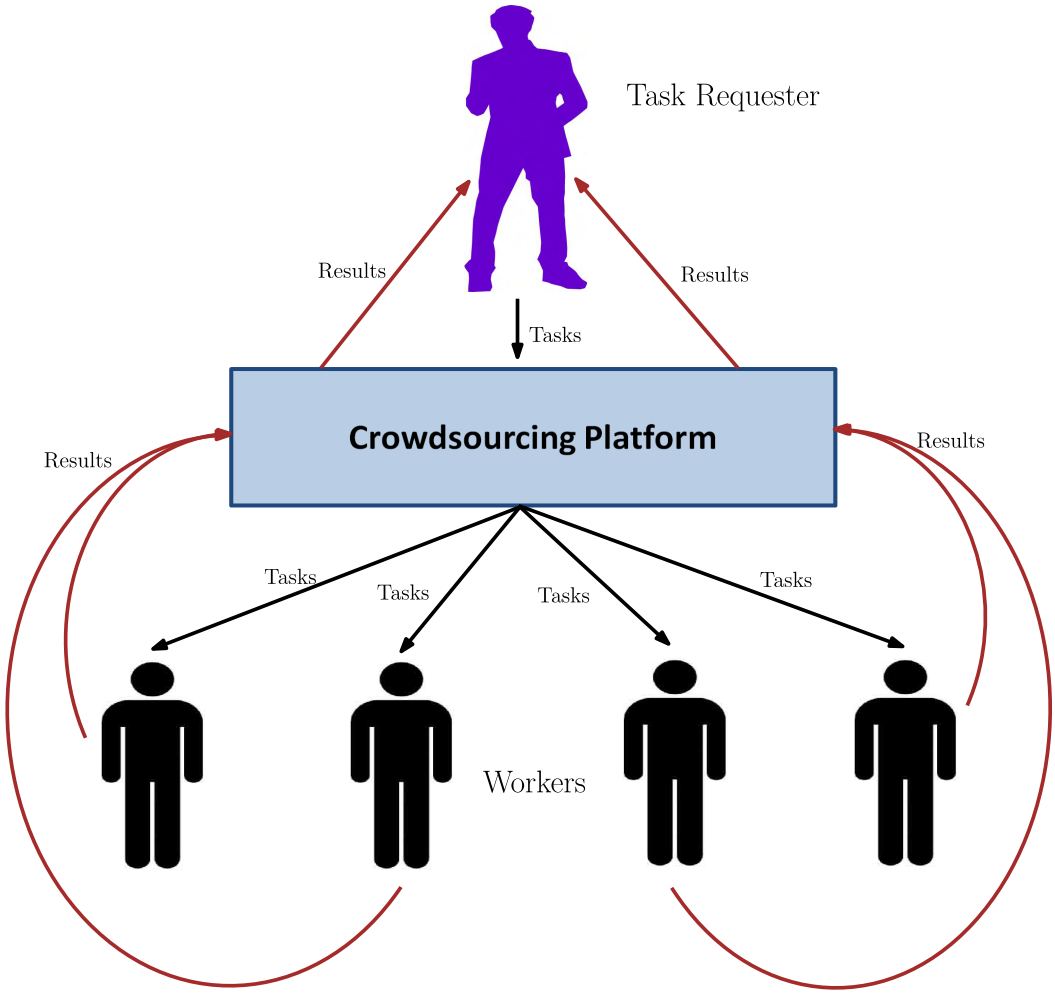

FIGURE 2. The crowdsouring practice consists of two types of users: task requester and the workers. The task requester distributes tasks to the workers through the platform, and collects the feedbacks from the workers in a reverse way.

enable individuals and business entities to use their own intelligence to perform tasks that are 'difficult' for automated computerized programs. Requesters post jobs or work in the form of human intelligence tasks on the MTurk platform, while workers browse the tasks and complete them to earn monetary incentives from the requesters.

Data privacy concerns limit the spreading speed of crowdsourcing because many users refuse to participate in crowdsourcing if personal data cannot be not securely protected. For example, when a requester evaluates the design of a particular artefact, it is likely that the requester desires to prevent exposure of the artefact. Similarly, a testing organization usually requires test takers not to disclose the content of the test. However, unlike a testing organization, which has the power to penalize test takers who violate the confidentiality agreement, the requester does not always have the power or effective methods to penalize workers who leak sensitive data or extract information for other purposes. What makes it worse is that the workers are sometimes unreliable and usually not identifiable. Therefore, it is challenging to protect the privacy of the requesters.

Generally, there are two approaches tackling the privacy protection problem for the requesters. The first solution, which is introduced by Varshney, distorts sensitive data directly using random perturbations to conceal private information [29]. A series of extensions were introduced by the same group of researchers for completing the framework based on coding theories [30]–[32]. The coding theory successfully hides the sensitive information from the workers. However, it loses the task performance quality when random perturbations are added to the original data. A mathematical model was used to analyze the tradeoffs between privacy, reliability, and cost, by considering five insight elements: error-correcting codes, reliability, perturbation, decoding and collusion attacks [33].

The second approach is the instance clipping protocol (ICP), which was introduced by Little and Sun [34] and Chen *et al.* [35]. Kajino *et al.* [36] proposed a quantitative analysis framework (QAF) based on the instance

TABLE 1. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdsourcing marketplace.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Varshney *et al.* [29], [33]	2012, 2014	Studying the tradeoffs between privacy, reliability, and cost	An improved coding scheme by considering five insight elements	Unable to solve the collision between privacy and task performance quality
Kajino *et al.* [36]	2014	Protecting the requesters' privacy defined as contextual information	Quantitative analysis framework based on instance clipping protocol	Making tradeoff between task performance and privacy
Celis *et al.* [37]	2016	Partitioning the task with minimal privacy leaks	The collusion network	Information leakage from the worker side
Amor *et al.* [38]	2016	Increasing the privacy awareness	SocialCrowd	Using heuristic function for optimal solution search, which can be trapped in worst case scenarios

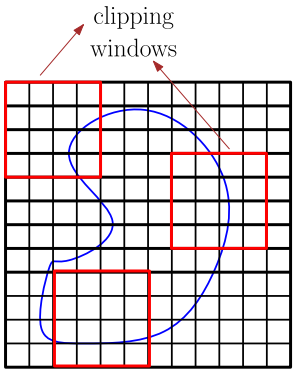

FIGURE 3. The instance clipping protocol: a task (represented by a 2D shape), is clipped by clipping windows which are marked by red boxes.

clipping protocol. The QAF evaluates the instance privacy-preserving protocols and protects the target privacy, which is defined as contextual information. The instance-privacy preserving protocols preserve instance privacy at the cost of task performance. For instance, in Figure 3, a task (represented by a 2D shape) is clipped by clipping windows which are marked by red boxes. Each worker is only allowed to access one clipping window for his/her task result. The ICP preserves privacy but decreases the quality of the task results. Similar to Varshney's work, there is a tradeoff between privacy preservation and task quality. The instance clipping protocol clips an instance by a moving window, which preserves the data privacy by limiting the data that each worker acquires.

Celis *et al.* [37] improved the clipping protocol by introducing a collusion network. The requested task is partitioned into pieces; and each piece of task is assigned to different individuals with minimal privacy leakage. Moreover, a framework is proposed with three operations: PULL, PUSH and Tug Of War (TOW). PULL and PUSH are two usual operations that represent a worker choosing tasks and a requester choosing workers, respectively. The TOW operation is used as an intermediate layer for information leakage minimization, which captures workers' personal information, such as social networks, financial information, task history and etc. However, information leakage is still possible from the workers' side.

Amor *et al.* [38] developed a social relationship management system based on clustering algorithms, named 'SocialCrowd', to manage competition and collaboration in crowdsourcing practices. Experimental results showed that the data leakage was effectively prevented using SocialCrowd. Since the first version of SocialCrowd uses global search algorithms, the main concern in Amor *et al.*'s work is the computational complexity problem. While a heuristic random search method is used in later versions, it can still be trapped into local extremes in worst case scenarios.

Table 1 lists all the references that we have discussed in this section, including their main objectives, proposed solutions, and weaknesses. In summary, while most recent studies of privacy protection in crowdsourcing marketplaces consider coding schemes or clipping protocols, new technologies, such as SocialCrowd, are proposed to help improve the data security. The common problem for the coding schemes and clipping protocols is that the manipulation of the original data decreases the task performance quality. Moreover, the extra time complexity that is added to the original data transmission and storage process is a notable issue for those efforts on privacy protection. In addition, while traditional works focus on protecting the requesters' data in a fundamental way, other issues are raised for improving users' awareness of privacy leakage during crowdsourcing practices. This will be further discussed in Section IV-A.

B. CROWDFUNDING

Crowdfunding has undergone fast development recently [39], [40]. It enables founders of various ventures to

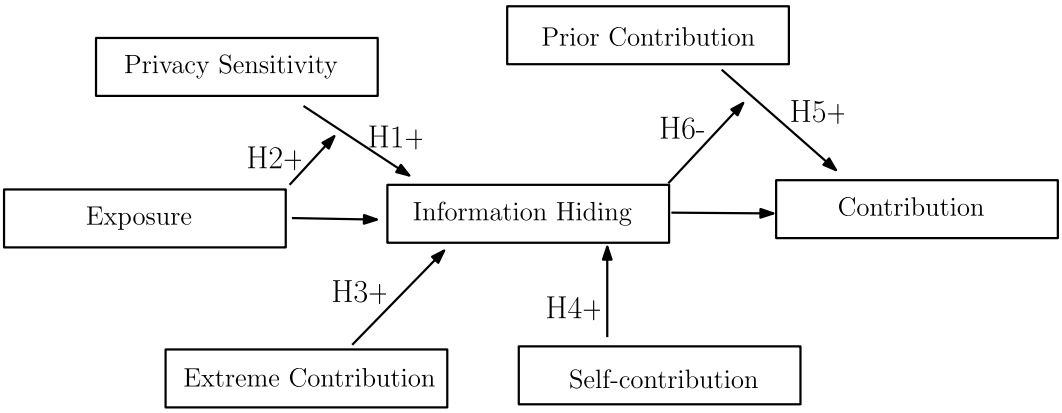

FIGURE 4. The econometric model proposed by Burtch *et al.* [44], [46]. The likelihood of information hiding and the amount of contribution from crowdfunders are affected by the six hypotheses shown in arrows. The six hypotheses are privacy concern effect (H1), exposure effect (H2), extremity effect (H3), self-contribution effect (H4), anchor effect (H5) and censorship effect (H6). The positive or negative effect is denoted by +/−sign.

fund their projects by collecting funds or other resources from a large group of individuals through an online platform, such as Kickstarter [41] or Indiegogo [42]. While most works focus on economic aspects of crowdfunding, few address privacy issues [43]. To bridge the gap between privacy concerns and practical use of crowdfunding, in this subsection, we review several existing works on privacy concerns in crowdfunding practices.

In the practice of crowdfunding, a fundraiser (the requester) proposes a project with a plan on an online platform and convinces users or supporters to invest small amounts of money in the project. The modern crowdfunding platforms, such as Indiegogo, allow users to customize their security level and conceal their personal information, such as their name and the amount of their contribution. However, our surveyed works suggest that revealing a certain amount of private information can be helpful in crowdfunding practice. For example, concealing the contribution amount of the prior contributor discourages followers from contributing more to the crowdfunding project [44]. Moreover, a fundraiser may choose to reveal more of his/her personal information to attract crowdfunders [45].

Burtch *et al.* [44], [46] conducted a series of experiments on a large-scaled customized crowdfunding platform to test the relationship between the privacy protection level and the results of users' contribution histories. An econometric model was constructed where the dependent variables included the likelihood of information hiding and contribution amount from crowdfunders. The independent variables included the privacy control of the fundraiser's platform, elapsed time of fundraising, and fundraiser's reputation. Six hypotheses were formulated: the privacy concern effect (H1), exposure effect (H2), extremity effect (H3), self-contribution effect (H4), anchor effect (H5) and censorship effect (H6). The econometric model is depicted in Figure 4, where the likelihood of information hiding and the amount of contribution from crowdfunders are affected by the six hypotheses, as shown with arrows. Although the econometric model provided valuable suggestions on privacy protection, it did not consider other factors that influence the crowdfunders' decisions, such as wording, information regulation, transaction mechanism design and etc.

In 2015, Burtch *et al.* [47] conducted another online experiment to study the hidden cost of protecting crowdfunders' privacy by utilizing modern techniques, such as invisible transaction information. Their result indicated that privacy protection increased the net funding in overall, but decreased the contribution amount from each individual. The main insufficiency of [47] is that all experiments and simulations were conducted in a randomized manner. Moreover, the users were given complete freedom for their fund contributions, which made the experimental result relatively unreliable.

Zheng *et al.* [48] analyzed the importance of trust management for crowdfunding practices. A research model was constructed for verification of five hypotheses. Experimental results showed that effective trust management techniques significantly improve the fundraising performance. Nevertheless, some important factors, such as funding information and presentation format of funding description, were not considered in the research model, which weakened the reliability of their conclusions.

Kang *et al.* [49] introduced a structural equation modeling technique to analyze the true motivations of fundraisers for crowdfundings. Three factors are considered to examine the trustworthiness of a crowdfunding project. The fundraisers' credentials were deeply analyzed by a bootstrapping method that is formed based on historical investment experiences. The main insufficiency of Kang *et al.*'s work is that the proposed method was not validated via any cross-sectional surveys.

All reviewed works for privacy issues in crowdfunding practices are listed in Table 2. Each reviewed work is accompanied by its reference, year, main objective, proposed solution and major insufficiencies. Certain levels of privacy

TABLE 2. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdfunding.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Burtch *et al.* [44], [46]	2013, 2014	Studying the relationship between security and willingness	An econometric model	Not taking the full consideration for factors that influence the crowdfunders' decisions
Burtch *et al.* [47]	2015	Showing the hidden cost of protecting crowdfunders' privacy utilizing modern techniques	Online randomized experiments	Experiment users are given complete freedom for their fund contributions
Zheng *et al.* [48]	2016	Analyzing the importance of trust management	A research model based on the elaboration likelihood model	Focusing on the trust management and ignoring other highly influential factors
Kang *et al.* [49]	2016	Revealing the fundraiser's true motivation for crowdfunding	A structural equation modeling technique	The survey dataset is small in size and limited to only one country

protection, as well as sacrifices, are hidden key factors for successful crowdfunding practices. With a well-established privacy protection protocol, crowdfunders are more willing to contribute because of a safer environment. However, in some situations, a certain degree of acceptable and controllable privacy sacrifice can be helpful for a successful crowdfunding practice. The fundraisers and platforms have to realize that the net funding is directly proportional to their reputations. One open problem is to develop a more sophisticated platform for protecting the funder information. For example, a hierarchical encryption system can be built to serve the basic crowdfunding purposes and allow the fundraisers to select different levels of information sharing with the public for various purposes. Another future research direction is to explore an appropriate degree of fundraisers' privacy disclosure that maximizes the probability of reaching a fundraising goal. Existing works showed that a certain degree of fundraiser's privacy disclosure encourages the funding contributions from users [50]. However, the most appropriate degree of fundraisers' privacy disclosure remains as an open problem for crowdfunding practices. Generally speaking, while crowdfunding is a relatively new concept to people in the cyber-enabled world and is directly related to assets, privacy issues are more emerging and are considered one of the most crucial research topics in the development process of the cyber-enabled world.

C. CROWDTESTING

Crowdtesting employs crowdsourcing technology to employ a large group of testers for software or products testing at low costs [51], which is reported to be more reliable, more cost-effective, and faster than traditional user-testing mechanisms [52], [53]. One popular crowdtesting platform is well-known as PyBossa [54], where customized crowdsourcing tasks can be posted, which require human cognition, knowledge or intelligence. The ultimate objectives of a crowdtesting practice include testing usability, acceptability, task performance and the quality of the results.

In a crowdtesting practice, both requesters and workers post crowdsourced data on an online platform, i.e., tasks and results. Part of the crowdsourced data can be privacy related, e.g., the data can include the requester's confidential data and tester's private information. The top priority for privacy preservation in crowdtesting is to protect user privacy in the data collection process. Harkous *et al.* [55] found that users usually had difficulties in accessing the privacy levels of their shared data. A context-aware framework was proposed to identify the privacy risk of shared data on a cloud server. Simulations on synthetic data were performed to show the effectiveness of their method, where data privacy levels were automatically assigned without user interaction. The main limitation of their work is that the proposed system only identifies the risky data items without proposing solutions. Moreover, there is no policy or computational technique proposed in [55].

Existing data protection schemes focus on encryption algorithms. Kandappu *et al.* [56] showed how easily privacy leakage can occur with online survey platforms, such as MTurk and Google Consumer Surveys [57], which are commonly used in crowdtesting practices. A customized survey platform called Loki was developed to let users choose their preferred security level before proceeding with the online survey. The actual survey results were masked by noises before been evaluated. There are two important insufficiencies in [56]. First, the result quality decreased because of the additional noises. Second, there was no guidance for the user to choose the most appropriate security level, which decreases the overall survey quality.

Li *et al.* [58] explored the privacy issues in crowdsourcing-based site survey systems utilizing WiFi fingerprint-based localization techniques. In a site survey practice, multiple suppliers were required to visit different locations and send

TABLE 3. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdtesting.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Harkous *et al.* [55]	2014	Identifying risking data pieces on cloud server	A context-aware framework based on item response theory (IRT)	Not discussing the way to protect privacy
Kandappu *et al.* [56]	2013	Allowing users to choose security level for online surveys	A customized survey platform called Loki	No guidance for the user to choose appropriate security level
Li *et al.* [58]	2016	Hiding the location information of the suppliers in indoor site survey practices	A homomorphic encryption scheme	The original measurement signal was distorted

back WiFi signals in a crowdsourced manner, which is similar to a crowdtesting practice. The main shortcoming of the work in [58] is that the location privacy protection of the suppliers is achieved by encryption and adding noises. The homomorphic encryption can distort the original measurement signal.

Although the crowdtesting service provides an innovative way for services/products to be tested by a large group of testers at low costs, the privacy issues were never well addressed to protect the sensitive information from both the requesters and the testers. Three specific applications of the crowdtesting practices are surveyed in this subsection: shared data protection on the cloud servers [55], online surveys [56] and indoor site survey practice [58]. The objectives, solutions and main insufficiencies are listed in Table 3. Almost all reviewed works demonstrate that user privacy can be easily breached by the service providers and platforms in crowdtesting practices. Various techniques were proposed to identify risky shared data and protect those sensitive information pieces. However, encryption or masking of the original data affects the usability of the final testing results, which limits the use of these cyber technologies.

D. SUMMARY AND DISCUSSION

In conclusion, in crowdsourcing practices, there are always three roles in the model: user, requester and platform. On one hand, the requester has the responsibility to protect workers' privacy. On the other hand, the requester designs mechanisms or protocols that discourage workers from leaking sensitive data of the tasks; and the workers are responsible for following the privacy agreements of tasks. The platform serves as a mediator that protects the privacy of both parties. Both the task requester and the users must understand that there are always tradeoffs between privacy and interests (e.g., incentives, task quality, funds). Both entities must sacrifice part of their privacy to enjoy a quality crowdsourcing practice. For example, in the crowdfunding practice, a reliable platform protects the privacy from both the users' and requesters' perspective, which increases the trust between both parties and further increases the chance of successfulness of the crowdfunding campaign [50], [59].

While most of the works that are surveyed in this section focus on cyber technology development on the platform for protecting the privacy of both the task requesters and workers, some policy/regulation works are mentioned as supplementary materials. Although the business models of these three crowdsourcing practice branches are different, raising the privacy protection level is always helpful to both the workers and task requesters in achieving their goals.

In general, on a crowdsourcing platform, users should be allowed to retrieve information from the database of a sharing service provider while the queries are maintained privately. In addition, to increase the security level of data protection for users, data de-identification methods are available in most cases [60]–[63]. Traditional methods, such as $k-$anonymity, $l-$diversity models, etc., can also be used to avoid linkage attacks [23], [64], [65].

III. PRIVACY ISSUES AND SOLUTIONS IN COLLABORATIVE CONSUMPTION PRACTICES

Unlike crowdsourcing-based sharing services, which combine the power of a large group of individuals to perform tasks, collaborative consumption allows individuals to access goods or services through P2P sharing that is coordinated by online platforms [5], [16]. In collaborative consumption practices, hosts provide shared goods or services through a collaborative consumption platform to customers. The sharing methods can be selling, borrowing, trading and sharing. Typical examples of collaborative consumption platforms include eBay (collaborative Online shopping), Uber (ridesharing) and Airbnb (homesharing) (Figure 5). Collaborative consumption has many benefits, such as greenhouse gas emissions reduction, cost saving, unaffordable goods access and decentralization [16], [66]. Although collaborative consumption has many advantages, it suffers from privacy concerns. In this section, we review problems and solutions related to privacy issues in collaborative consumption.

A. COLLABORATIVE ONLINE SHOPPING

Online shopping is probably the first successful model in which cyber technology has changed our living world. In the

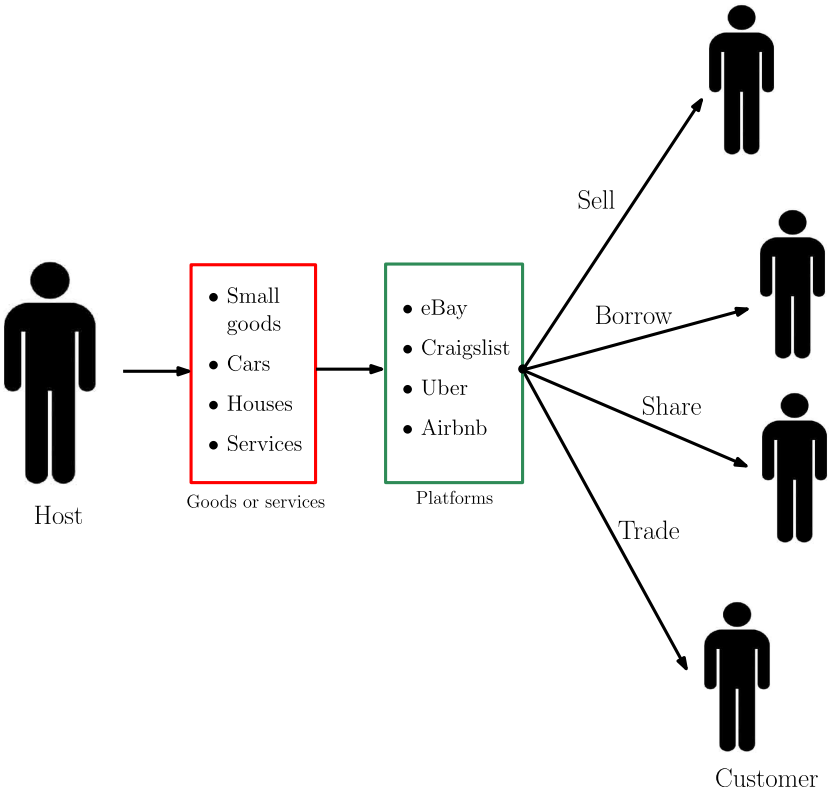

FIGURE 5. A typical demonstration of collaborative consumption: hosts provide shared goods or services through a platform to the customers. The sharing methods include selling, borrowing, trading and sharing; the typical examples of collaborative consumption platform include eBay, Craigslist as well as Uber (ridesharing) and Airbnb (homesharing).

first stage of online shopping development, people found that it was more convenient and economical to purchase goods over Internet. In the process of cyber technology development, the concept of collaborative consumption was gradually embedded into the online shopping experience. People started to sell small items, trade services, share cars and borrow items through online shopping websites [16].

On the other hand, online shopping websites have received many criticisms due to their notorious privacy policies despite their popularity [67]–[70]. Although it is illegal to reveal user information to third parties without user consent, online platforms are not subject to a penalty for analyzing user data. These platforms rely on third-party organizations for data analysis, which deteriorate customers' privacy. The privacy policy terms are supposed to be accepted by customers without negotiations, which are in some sense unfair to the customers. Except for limited government regulations, these marketplaces are self-regulated or autonomous, which makes it difficult to protect consumer's privacy. Moreover, these platforms suffer from data leakage due to cyber attacks or intrusion. These factors contribute to the vulnerability of consumers' privacy.

Miyazaki and Fernandez [71] surveyed about online shopping fears on a set of U.S. Internet users from different age groups, economical classes and educational backgrounds. The survey results indicated that the untrusted security system is the largest fear of the customers. Malhotra *et al.* [72] systematically analyzed Internet users' information privacy concerns (IUIPCs) through two separate surveys of 742 household respondents. They designed a theoretical framework for studying IUIPCs and proposed a causal model that predicts the reaction of online customers to privacy threats from shopping websites. Tsai *et al.* [73] studied how the privacy concerns of customers affected their decisions in the online shopping process. They conducted an experiment to test the shopping decisions that were made by customers after displaying their personal information on the shopping websites. Their results demonstrate the customers' willingness to pay a premium for extra privacy protection (from a more expensive shopping website). All of the above mentioned works reveal the fact that the privacy concern is the main fear in online shopping experiences. However, these works do not present a deep analysis on how to build privacy protection trust between online shopping websites and customers using regulation policies or cyber technology.

Shiau and Luo [74] built a research model using partial least squares (PLS) method to analyze the relationship between consumer satisfaction, intention of online group buying and user beliefs (Figure 6). The PLS results show that consumer satisfaction highly depends on trust, followed

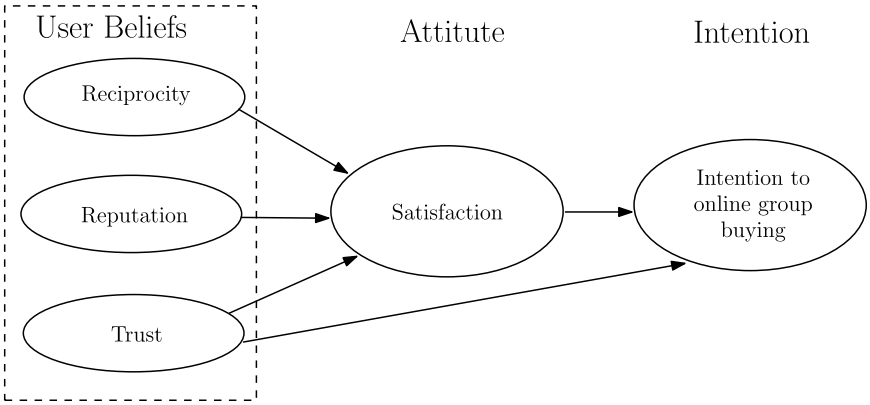

FIGURE 6. The research model proposed by Shiau and Luo [74], showing the relationship between consumer satisfaction, intension of online group buying and user beliefs.

by reciprocity. It is the first work to draw an overall picture of the different factors that affect the online shopping decisions. Moreover, it is also the first work to clearly identify privacy concern as the first priority for online shopping security. Following Shiau and Luo's work, Bergström [75] built an analytic system with different groups of people concerning various privacy issues in online shopping experiences. Both the customers and the privacy concerns were partitioned into different dimensions to interpret the links between socialization, Internet experience, trust, politics, and security understanding. Their analysis result clearly indicated that the trust is the major concern of people who worry about the misuse of personal data. Although these research models go one step further than the simple survey results, they still do not provide a clear solution for protecting the customers' privacy in online collaborative shopping practices.

Preibusch *et al.* [76] studied and reported a concrete example of privacy leakage in online shopping practices. They performed online tracking and found that online shopping websites send unnecessary personal information to payment providers, such as Paypal. Therefore, there is an on-going risk for customers who shop online. The most effective method for changing this situation is to facilitate relevant legislation. However, the lack of government regulation of online shopping websites exists globally. Moreover, it remains unclear what rules can be added and how they can be enforced. Although there are existing regulations (Directive 95/46/EC by the European Union [77] and USA Patriot Act [78]), existing studies have shown that those regulations are usually ignored due to insufficient government monitoring.

One solution to protect users' privacy in collaborative online shopping practices is to install third-party privacy protection software in the web browser. Available software on Internet includes the Tor Browser [79], the Privacy Bird [80] and the Platform for Privacy Preferences [81]. These third-party software programs or plugins identify untrusted shopping websites and mask personal information for the customers. However, third-party software is usually not formally authorized or registered by the government, which potentially raises other concerns of privacy leakage.

Lee *et al.* [82] proposed a π-box mobile app to control the sensitive data transmission between different users and from users to service providers. The π-box extends the user apps and was built based on the cloud services that were supplied by large companies, such as Google. Two separate channels were designed: the sharing channel, which controls the data transmission between users and the aggregate channel; and the aggregate channel, which controls the data transmission from users to the service provider. The structure of π-box is illustrated in Figure 7. All channels are internally monitored by a centralized system. The limitation of the proposed π-box is that it does not universally apply to any app in market. According to a user survey conducted by Lee *et al.* [82], only 48% of paid apps support π-box, which limits its usage on privacy protection.

Kokolakis [83] studied the conflict between the customer's high demand for privacy protection and the customer's willingness to sacrifice privacy for the exchange of goods or services in the online shopping practice. Kokolakis concluded that this inconsistency represents a collision between a customer's attitude and behaviour, which is known as the privacy paradox [84]. A large volume of works was surveyed to justify the existence of the privacy paradox; however, most of them are surveys or experimental works that do not involve theoretical model.

Bilge and Polat [85] introduced a method for improving the online shopping experience by collecting customers' personal information, such as ratings and comments for a particular service, in a privacy-preserving manner. A number of clustering methods were integrated into the collaborative filtering service. The system filtered out customized information by training on encrypted user data using clustering methods. The main insufficiency of the work in [85] is that, due to the encryption of the users' data, the recommendation error rates increased. In addition, the clustering methods introduced extra computational costs to the recommendation system.

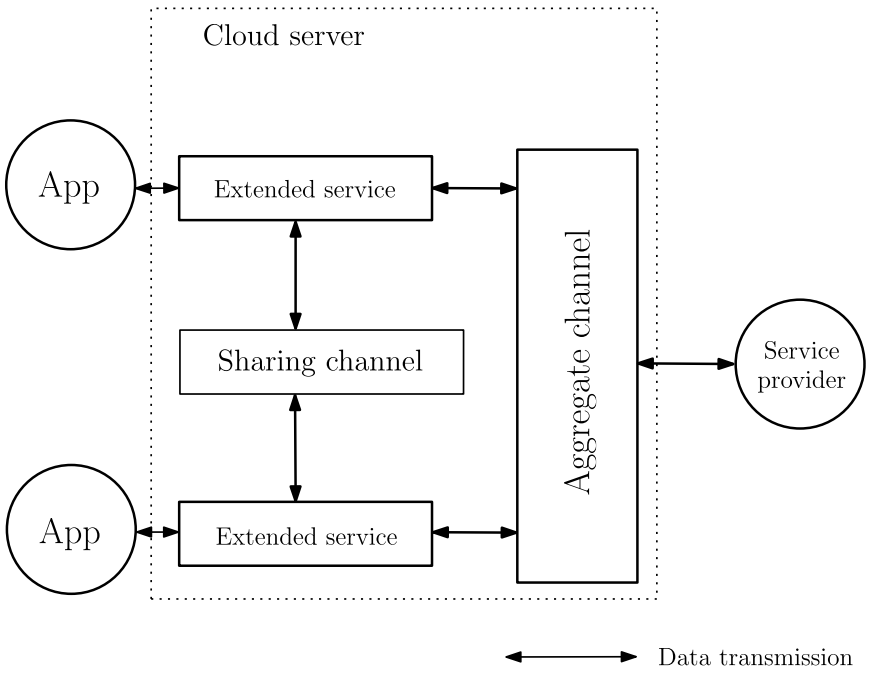

FIGURE 7. The internal structure of π-box: it extends the user apps on cloud server. Two separated channels were designed, which were the sharing channel controlling the data transmission between users and the aggregate channel controlling the data transmission from users to the service provider.

TABLE 4. References, main objectives, proposed solutions and important insufficiency of the surveyed works for collaborative Online Shopping.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Miyazaki and Fernandez [71], Malhotra *et al.* [72], Tsai *et al.* [73]	2001, 2004, 2011	Pointing out the biggest fear for online shopping experiences	Surveys on Internet users	Lacking a deep analysis to build the privacy protection trust between the online shopping websites and the customers
Shiau and Luo [74], Bergström [75]	2012, 2015	Learning the largest privacy concern in online shopping practices	Drawing the overall online shopping fears relationships by research models	No clear solution for protecting the online customers' privacy
Preibusch *et al.* [76]	2016	Pointing out the need of raising governmen-t regularization for online shopping globally	A concrete example of the privacy leakage in online shopping practices	What rules to be added and how to add are two big questions
Lee *et al.* [82]	2013	Separating the data transmission from user to user and from user to service provider	A mobile app called π-box	Not supporting all paid apps
Kokolakis [83]	2017	Revisiting the conflic-t known as 'privacy paradox'	A survey covering related existing works	No theoretical model was discussed
Bilge and Polat [85]	2013	Protecting privacy in user information collection process for a recommend system	Masking sensitive data and using clustering methods for data analysis	Losing analysis accuracy

The reviewed works, which are listed in Table 4, identified two privacy threats in collaborative online shopping practice. The first threat comes from the service provider, where unreliable platforms may misuse customers' data for marketing analysis. This threat can be prevented by refining government regulations [76], masking customers' data

before sending them out [85] or separating communication channels on the cloud server [82]. Other possible solutions to prevent such malicious behaviours include utilizing trusted computing [86] or building services based on a trusted provider [87], [88]. The second threat comes from the customer side, where most customers realize that they must sacrifice a certain degree of privacy to enjoy the collaborative shopping experience [83]. It is difficult for them to choose a trustworthy service provider, products [75], and most importantly, the kinds of permissions to grant [89]. The second threat can be alleviated by increasing the overall privacy awareness of the users, which will be extensively discussed in Section IV-A.

B. RIDESHARING

Real-time ridesharing or dynamic carpooling is a transportation service that allows commuters to share rides on very short notice through mobile apps [90]–[94]. Successful ridesharing platforms, such as Uber, are available in most major cities in the world. When a user needs a ride, he/she may simply use a mobile app to request a ride by entering the destination. The app provides the estimated cost and assigns a driver to the passenger. The payment is generally made with the credit card or other digital payment methods that are associated with his/her account. In the end, both the passenger and the driver will rate each other.

It is well known that the mobile apps can track the customers' location information and travel information for better service quality. The driver has to access to the rider's travel information, such as riders' names, trip starting points and destinations to provide services. Under current privacy policies, riders have to share part of their private information to receive ridesharing services. The platforms have limited regulatory power over the drivers because the drivers are contractors rather than employees of the ridesharing companies. Moreover, drivers' names and license plate information are also subject to disclosure. Concerns have been raised about the internal misuse of user data within the ridesharing companies. For instance, staffs in the ridesharing companies have the access to data for tracking the movements of customers. Taking Uber as an example, in its user agreement terms, it is clearly stated that user information, such as the geo-location, is recorded and internally used by the company for research development purposes. However, the purposes of internal research are not defined explicitly. Customers worry about how their private data is used. Additionally, Uber can access, use, preserve, transfer and disclose user information to prevent, discover or investigate violations of the privacy policy or the user agreements as determined necessary or appropriate. However, customers do not know what information is necessary or appropriate.

Location privacy has been studied extensively in recent decades because of the pervasiveness of geo-location related software and mobile apps [95]–[99]. While location-aware applications track customers' location or other data online, they generate a huge amount of potentially sensitive data. The privacy of location data depends on the regulation of data access. It is neither necessary nor possible to forbid all accesses because the systems must access the data for analysis purposes. Moreover, access permissions should be given to authorized persons and should never be exposed to others. In other words, the data and the access should be tightly controlled and data should be accessed only with legal authorization [95].

Kido *et al.* [100] proposed one of the first techniques for concealing the actual locations of customers in location-based services, including ridesharing practices. When a user sends an inquiry to the server, he/she sends his/her actual location, together with two false positions called 'dummies.' The dummy nodes in the tracking system are carefully generated such that an observer cannot easily identify the actual location of the user; however, the location-based server (LBS) can find the difference through optimized algorithms with external information such as road navigation service (RNS) data. The obvious shortcoming of Kido *et al.*'s work is that the real location is not completely concealed (by using dummies). There is still a chance that the observer will identify the actual location.

Yao *et al.* [101] provided an effective encryption service for ridesharing customers using the clustering k-anonymity (CK) scheme [23]. The CK scheme encrypts the user location information by utilizing a cloaked spatial-temporal boundary (CSTB) that involves K users. The spatial and temporal constraints, which determine the resolution of the encryption, can be customized by users. However, the use of CSTB decreases location information resolution, and consequently, degrades the service quality of ridesharing.

Pan and Meng [102] extended Yao *et al.*'s work using a p-anti-conspiration model for location privacy protection. Various techniques were introduced, including methods that provide LBS without knowing the actual locations of the customers. It is a large advancement for the ridesharing companies in protecting the user locations. A follow-up work done by the same group of Pan *et al.* [103] showed that the approach proposed in [102] lacks protection on sensitive information during the data transmission process.

Jagwani and Kaushik [104] intended to prevent location information leaks using the concept of Zero knowledge proof (ZKP). The construction process of the authentication scheme based on ZKP was introduced; and the possible applications of ZKP in the location-based service domain were discussed. The main shortcoming of the ZKP approach is that an authentication scheme is always required to coordinate between customers and hosts.

Gao *et al.* [105] introduced trajectory privacy in the ridesharing practices. The trajectory privacy contains spatial-temporal information, which is an important addition to the location privacy protection scheme. In their study, they proposed a mixed-zone graph model to protect the trajectory privacy. The actual implementation relies on a third party

middleware, where the actual location information leakage exists.

In recent years, online social networks or geosocial information have started to be used in ridesharing services. It is preferable to use a friend's car rather than stranger's. Based on this motivation, Elbery *et al.* [106] proposed a social Vehicular Ad-Hoc Network (S-VANET) carpooling recommendation system. They embedded friendship locality, preference locality, and travel locality information into the ridesharing recommendation system, which requires a large amount of privacy information from both the requester and his/her friends.

Ni *et al.* [107] suggested that customers' true identities can be hidden by incorporating an anonymous mutual authentication (AMA) protocol into the carpooling recommendation system. A real-time navigation system is proposed for concealing the drivers' privacy [108]. One important feature of their application system is the false information traceability, where the trusted third party authority can trace incorrect information, either from a user or a driver. The main limitation of their work is that a trusted third-party middleware is still required.

Aïvodji *et al.* [109] proposed a privacy-preserving local computational method for determining the meeting point of a driver and a rider in a ridesharing system, which does not require third-party middleware. Multimodal routing algorithms are used to compute a mutually interested meeting point for both the driver and rider. However, the current developed system was only designed to accommodate one driver and one rider. A more sophisticated system that can include multiple drivers and riders for ridesharing practices is left as a future work.

Shokri *et al.* [110] concluded that the current location privacy protection approaches can be concluded on three trends, which are perturbing the actual location, tracing the perturbed location, and evaluating the privacy-preserving methods. While most existing works only focus on encrypting the customer's current location, strategies were employed by attackers to trace down the actual location of the customer. Useful private information pieces, such as recently visited locations, frequently visited places and nearby landmark buildings, become potential clues for the attackers in estimating the current location of the customer. In [110], a comprehensive Bayesian security game is designed to simulate various cases in which a strategic attacker traces the actual location of a customer. Four different scenarios were studied. However, it was difficult to predict the intelligence level of the attacker; and the whole simulation system is too complex in most of the real-world scenarios.

Vergara-Laurens *et al.* [111] categorized privacy preserving systems into approaches for two processes: the tasking process, where tasking devices (such as mobile phones) collect data in certain areas; and the reporting process, where distributed devices report sensed data to the platform. Both processes exist in ridesharing practices. Three open problems were raised for crowdsensing (CS) researchers in the field of location privacy preservation, which are 1) privacy-preserving mechanisms for tasking processing, 2) privacy-preserving mechanisms for reporting process and 3) selecting the most appropriate privacy-preserving mechanism.

Wang *et al.* [112] proposed a two-stage auction algorithm taking both trust degree and privacy sensibility into consideration for mobile crowdsourcing systems, such as ride-sharing practices. The k-anonymity scheme is integrated with ϵ-differential scheme to add Gaussian white noise to the actual locations of users. The proposed scheme was proven to be trustful and can inspire more users to participate in the mobile croudsourcing systems. Insufficiency exists while the added Gaussian white noise increases the computational complexity and consequently weakens the service quality for mobile crowdsourcing systems.

All reviewed papers are summarized in Table 5. Similar to other sharing services, customers realize that a certain degree of their privacy must be sacrificed to enjoy better service quality. Taking the Uber service as an example, the platform (Uber app) usually records the customers' private information, including current location, destination, phone number, recent trips and so on, to serve them better. However, the customers sacrifice their privacy to enjoy the Uber service. The conflict between the disclosure of private information and the service quality becomes more obvious in the ridesharing practices, which is also mentioned in most of the surveyed works, such as [105] and [108], [109], [111].

Compared to other fields of sharing service, ridesharing is a relatively new technology. Few regulations have been established in this area; and most privacy concern solutions are on technical aspect. Despises the variety of technologies proposed by the existing works, only location privacy is extensively discussed. Ridesharing services include direct interpersonal interactions (IPIs), e.g., the conversation between the rider and the driver when they are travelling [113]–[115]. Computerized technologies, which are designed to be embedded in the online platform, can be helpless in IPI; and physical privacy concerns exist at this stage [15]. Physical privacy concerns, which were first defined by Belk, occur when the driver or passage's personal space is invaded, where we refer to the remaining privacy concerns as online privacy concerns [116], [117]. For future works in this field, we would like to note that physical privacy protections for both the riders and drivers are demanded in the ridesharing practice.

C. HOMESHARING

Homesharing is a business model that connects hosts and travellers through an online marketplace platform and enables transactions without the platform owning any rooms itself. It does not provide the rental services directly. Instead, it matches hosts who have extra rooms for rent and travellers who need a room for stay [118], [119]. One of the most famous homesharing platforms is Airbnb [120].

The face-to-face e-commerce model makes the physical privacy issue more serious for homesharing practices

TABLE 5. References, main objectives, proposed solutions and important insufficiency of the surveyed works for ridesharing.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Kido *et al.* [100]	2005	Protecting location privacy using dummies	An anonymous communication technique	The actual location is not completely concealed
Yao *et al.* [101]	2010	Encrypting the user location information	Clustering K-anonymity (CK) scheme	Decreasing location information resolution and degrading the QoS
Pan and Meng [102]	2013	Providing location-based services without knowing the exact location	The p-anti-conspiration privacy model	lacking protecting sensitive information
Jagwani and Kaushik [104]	2012	Removing the dependency of using third party software	Zero knowledge proof	An authentication scheme is required
Gao *et al.* [105]	2013	Protecting the trajectory privacy	A trajectory privacy-preserving framework	The exact location must be revealed to a third party middleware
Ni *et al.* [107], [108]	2016	Concealing both customers and drivers' sensitive information	An anonymous mutual authentication (AMA) protocol	A trusted third party middleware is required
Aïvodji *et al.* [109]	2016	Computing the mutually interested meeting point	Multimodal routing algorithms	A more complicated system involving multiple drivers and riders are left for future exploration
Shokri *et al.* [110]	2016	Considering strategic attackers for customer's location privacy	A comprehensive Bayesian security game	The complexity is not necessary for most of the real-world scenarios
Vergara-Laurens *et al.* [111]	2017	Surveying privacy-preserving mechanisms	A survey of all existing works on location privacy preservation	Only location privacy is heavily surveyed
Wang *et al.* [112]	2018	Inspiring more users to participate in the mobile croudsourcing systems	Integrating k-anonymity scheme with ϵ-differential scheme	The addition of Gaussian white noise weakens the crowdsourcing service quality

compared with online sharing model. The host and traveller usually meet each other before a deal was made and both of them have the possibility to reveal the privacy of each other to the public. For example, a host may install a hidden camera in an Airbnb room to monitor travellers. A traveller may take pictures to reveal the details of the room or other parts of the house to the public. The online platform records sensitive information of both the hosts (e.g., names, travel plans) and the travellers (e.g., names, home locations).

Kamal [121] realized that the largest inhibitor of homesharing services is the fear of privacy disclosure. They argued that additional background checks are always necessary for participants in homesharing activities, with the possibility of additional security measures, such as certificates and safety insurance. However, we would like to point out that the cost comparison between the additional security checks and the actual accommodation is not discussed in [121].

Morosan and DeFranco [122] determined the level of willingness of travellers to disclose their personal information to hotel apps. An extended version of the privacy calculus model was adopted. The experimental results indicated that personal information disclosure was indeed helpful for the hotel business, i.e., to choose the best customers. But the willingness of disclosing such information was related to privacy concerns, trust, emotions and etc. The main insufficiency of this work is that the study data was collected from U.S. customers who were involved in a relatively safe environment with reliable network security, regulations and hotels. The experimental results may not be applicable to third-world countries.

Ert *et al.* [123] designed an experiment that used mixed-logit analysis to determine the relationship between the posting of a host's photo in the advertisement and the booking likelihood. The results show that both the trustworthiness and attractiveness of the host's photo increase the likelihood of the house being booked. Similar to crowdfunding and crowdtesting, an appropriate degree of private information disclosure from the hosts's side increases the probability of success for the entire practice/business. However, on the

TABLE 6. References, main objectives, proposed solutions and important insufficiency of the surveyed works for homesharing.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Kamal [121]	2016	Building trust in homesharing practices	Proposing additional security checks	Not discussing the cost of additional security measurements
Morosan and DeFranco [122]	2015	Checking the willingness of hotel customers to disclose personal information	An extended version of the privacy calculus model	Collecting data only based on U.S. customers
Ert *et al.* [123]	2015	Showing the relationship of posting a host's photo and the booking likelihood	Mixed-logit analysis	The relationship between trust and privacy is of interest but not discussed
Lutz *et al.* [125]	2017	Investigating the impact of physical privacy concerns to homesharing	A survey on MTurk	Only hosts were surveyed

other hand, the leakage of the hosts' privacy, including posting of the host's photo and identity information, is another issue in homesharing practices, which is deeply discussed by Hooshmand [124].

Lutz *et al.* [125] explicitly divided the privacy concerns into physical privacy concerns (e.g., physical damages of private assets) and online privacy concerns (e.g., personal identity leakage). They conducted a survey on MTurk involving 389 participants; and most of them were hosts on Airbnb. The survey results showed that physical privacy concerns are more crucial than online privacy concerns in the homesharing business. The main shortcoming of their work is that the survey is limited to Airbnb hosts and does not include any customers. Thus, the survey results may be biased towards the hosts' preferences.

We list all reviewed works for security concerns of homesharing in Table 6. Similar to crowdsourcing practices, certain degrees of private information disclosure from the hosts side positively influence the trust from the customers side and consequently attract more customers. Moreover, compared to other sharing services, homesharing involves more interpersonal interactions. Concerns about physical privacy are heavily studied in this field. Most of our surveyed works agreed that the hosts are more concerned about their privacy leakage than the travellers. Future studies can focus more on the development of privacy protection schemes for hosts. In the current stage of homesharing, while it is unlikely to solve the privacy issue with a single method, it is quite possible to provide a general privacy-preserving environment for both hosts and travellers through the joint efforts of hosts, travellers, platforms, and governments.

D. SUMMARY AND DISCUSSION

Collaborative consumption collects extra information resources and distributes them to people who do not have access to them. Users are subject to privacy leakage due to the exchange of data and improper use of user data by internal staffs or the platforms. Similar to crowdsourcing practice, both hosts and customers must understand that certain degrees of their privacy have to be sacrificed for better service quality. The most appropriate degrees for private information disclosure from both hosts and customers side are left as open problems to maximize the service quality and net profit. While it is difficult to provide an absolute privacy-safe environment without sacrificing service quality, it is possible to increase the protection levels of privacy through a joint effort of all participants, platforms and governments [75], [76], [82], [83], [85].

Compared with collaborative online shopping, both ridesharing and homesharing involve more interpersonal interactions (IPIs). For ridesharing, location privacy is separated from the general concept of privacy and is extensively studied and discussed. For homesharing, the general form of privacy is further divided into online privacy (electronic forms of personal information) and physical privacy (human body, house, furniture, etc.) [15]. There are works showing that the physical privacy concerns are more important than online privacy concerns for homesharing [117], [125]. We believe that the concept of physical privacy will be considered in privacy protection studies in other areas in near future, such as ridesharing.

It is noted that there are other methods available for privacy preservation in collaborative consumption practices in the early years. Milberg *et al.* [126] studied various aspects that affected the customers' willingness to participate in collaborative consumption in the early 1990s. The study shows some early efforts and results from governments in designing suitable regulations for protecting the customers' privacy. Luo *et al.* [127] examined several mechanisms to demonstrate the close relationship between trust and privacy preservation. Nissenbaum [128] discussed privacy from the perspective of contextual integrity in technology, policy, and social life.

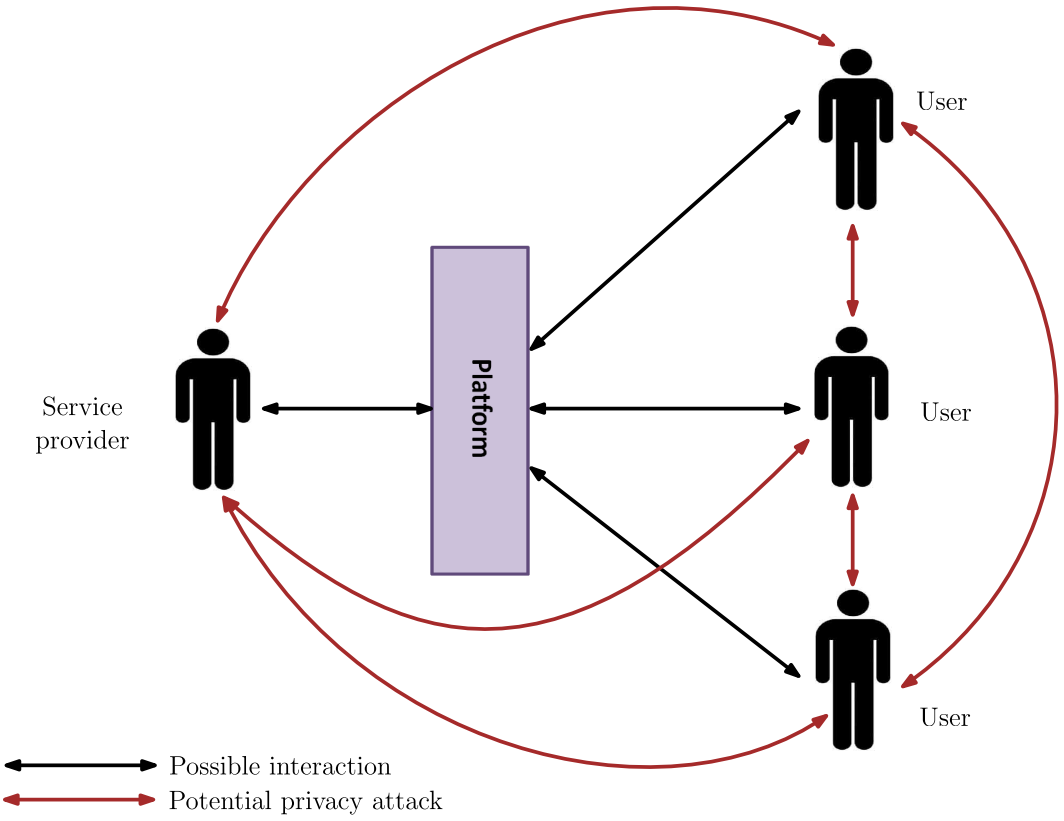

FIGURE 8. The privacy relationships between the user, platform and service provider. For any participant in the sharing practice, no matter he/she is a user or service provider, all the remaining people involved in the same sharing practice can be potential attackers to compromise his/her privacy.

IV. SUMMARIZING EMERGING PRIVACY ISSUES FROM THE USER, PLATFORM AND SERVICE PROVIDER PERSPECTIVES

Fast development of cyber technology facilitates the invention of novel sharing practices in the cyber-enabled world. While traditional privacy problems have either been solved or at least realized by the government and society, privacy issues in cyber-enabled sharing services are less understood. In all six branches of the taxonomy in Figure 1, there are always interactions between users, platforms, and service providers.

In this section, all existing privacy issues are further discussed from three perspectives, namely, users', platforms' and service providers' perspectives. we argue that all privacy issues from different applications are internally related. Users concern with their own privacy and always demand high quality reliable sharing services. Service providers realize that privacy security level is a key element towards a successful achievement. Anybody involved in the sharing service can be a potential attacker to compromise other people's privacy. The linkages between the privacy concerns from the three perspectives are shown in Figure 8. The concluded emerging issues of the cyber-enabled sharing services are: increasing users' privacy awareness from their perspective, protecting shared information from the platforms' perspective and making privacy concerns the top priority from the service providers' perspective. Works that are surveyed in this section are listed in Figure 9 and summarized from the three perspectives.

A. FROM USERS' PERSPECTIVE: INCREASING PRIVACY AWARENESS

Although most websites, software and mobile apps provide user agreements for user privacy awareness, only a negligible portion of users read through the tedious clauses carefully. The first emerging privacy issue for cyber-enabled sharing services is to maximize users' awareness of privacy leakage, e.g., to provide an online tool for users to trace down entities that may reveal their personal information. The transparent information tracing system will increase the confidence of users in participating in sharing practices on Internet, as well as facilitating the service providers to improve their reputations.

For example, in the crowdsourcing marketplace, it is not sufficient to protect only requesters' data privacy because workers also value their privacy equally. Workers are commonly afraid of the leakage of their location data or the identity information (e.g., age, contact, hobbies, activities) [129], [130]. According to a survey that was performed by the U.S. Federal Trade Commission [131], more than 85% of users were too impatient to read the user agreements regarding privacy settings carefully. They were surprised that

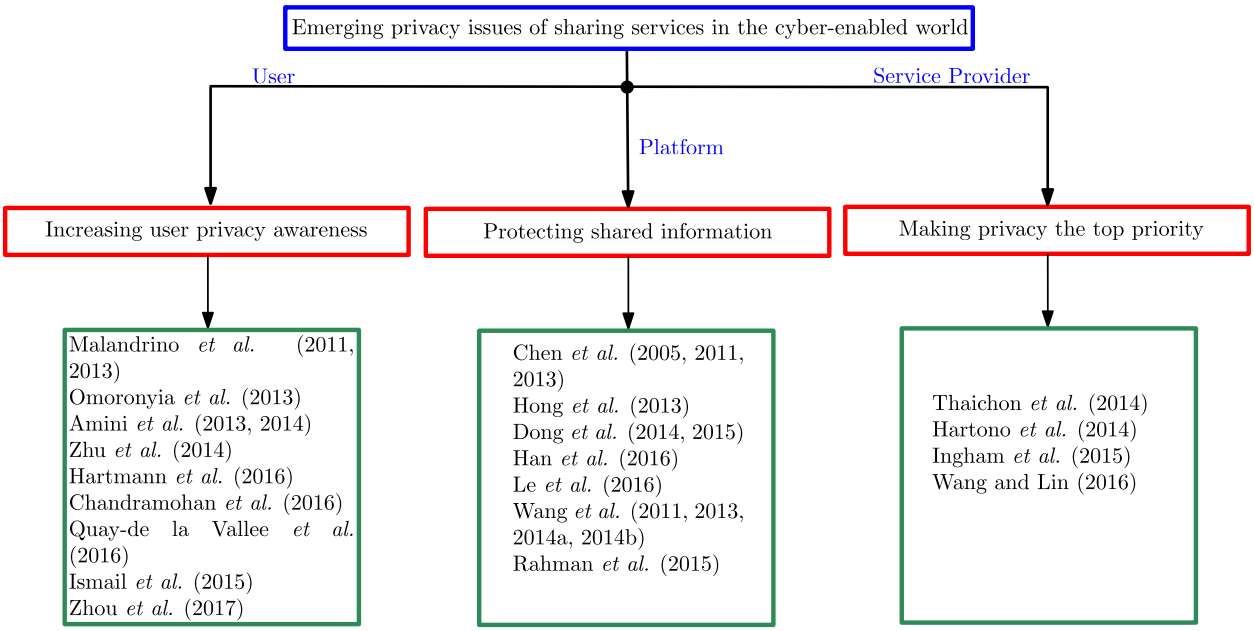

FIGURE 9. The emerging privacy issues identified in the current stage of cyberized sharing service development from the user, platform and service provider perspectives. The emerging privacy issues are shown in the red boxes. All works surveyed in this section are listed in the green boxes.

mobile phone apps sent their approximate or precise location, phone's unique ID to service providers. Some apps even have control of the camera flashlight and audio settings. Although these privileges were authorized by users, they did not know when or where they give the authorizations, because they never read the articles about the privacy settings. Some efforts have been made to solve the above problem.

Malandrino and Scarano [132], Malandrino *et al.* [133] proposed a privacy awareness software named 'NoTrace' to provide privacy recommendations to the users, such as privacy protection level settings, private information transmission warnings and unnoticeable privacy leaks warnings. The graphical user interface of 'NoTrace' clearly displays the private information pieces that are received by the service provider. The main shortcoming of Malandrino *et al.*'s work is that they did not provide a deep analysis of which private information pieces are necessary for the service quality and therefore, could not provide proper recommendations on selective disclosure of personal information for users.

Omoronyia *et al.* [134] proposed an adaptive privacy framework to assist automatic privacy disclosure decision making for various applications. The framework is designed following the famous MAPE (Monitor, Analyse, Plan and Execute) loop, and is focused on three aspects: application attributes, potential privacy threats and derived benefits from privacy disclosure. One important insufficiency of their work is that it does not categorize privacy protection requirements according to different service functions, which makes the automatic privacy disclosure decision making relatively unreliable [135].

Amini [136], Amini *et al.* [137] developed a software called 'AppScanner' to help users better understand the functionalities of mobile applications. The software provides an informative description of what mobile apps are actually doing under a crowdsourcing environment. The transparency and detailed analysis of the mobile apps help make users aware of privacy leakage when using mobile apps for crowdsourcing. AppScanner only categorizes the mobile app behaviors as normal or abnormal. A detailed categorization according to the behaviors purposes, e.g., advertising and social networks, can be used to enhance the decision making ability for users [138].

Zhu *et al.* [139] implemented a mobile app recommendation system with security and privacy awareness. The proposed system first analyzes the mobile application with detection and diagnosis of the security risks from insecure data access permissions. The recommendation system then provides suggestions to the user on whether to continue using the mobile app according to the app's popularity and user settings. The recommendation is based on modern portfolio theory. The main insufficiency of Zhu *et al.*'s work is that the security risks are only evaluated based on the permissions that the mobile apps request.

Hartmann *et al.* [140] summarized six main threats of mobile apps to make the users aware of potential privacy risks: insufficient control features, excessive data mining, data theft, surveillance, information leakage and social engineering. They also proposed eight recommendations for guarding against these privacy threats: privacy dashboard, privacy policy, data handling guidelines, user permissions, anonymization, IT infrastructure security, encryption, and relationship. All the guidelines are valuable for future privacy-aware mobile application development. However, most importantly, immediate solutions for all

conflicts are missing from both regulation and cyber technology perspectives.

Chandramohan *et al.* [141] concluded that over 90% of users accept user agreements unconsciously, without knowing that their personal information can be misused. They described a complete privacy-preserving scheme called Petri-net Privacy-Preserving framework that was installed on a cloud server. However, the practicability and the scalability of their algorithm are still questionable.

Similar to traditional websites that force users to accept user agreements, the mobile apps mitigate the privacy risks to the users by requesting resource access permissions. Quay-de la Vallee *et al.* [142] developed two app systems that help users find privacy-respective apps and manage the apps' permissions in their mobile phones. The main shortcoming of Quay-de la Vallee *et al.*'s work is that the two systems only provide privacy management assistance after the apps have been installed, instead of providing the assistance during the installations process.

Ismail *et al.* [89] studied the privacy threats from mobile apps that require access to sensitive resources during the processes of installation or updating. A crowdsourcing strategy that identifies the minimal number of permissions to keep the mobile apps fully functioning for a diverse range of users was proposed. A user study that involved 26 participants and the popular mobile app 'Instagram' showed the effectiveness of their approach. However, the survey size was relatively small; and the method was only tested on a single mobile app. The usability of the proposed crowdsourcing strategy requires further justification.

Zhou *et al.* [143] accessed the gap between users' desire of privacy control and the actual privacy setting functions provided by mobile app systems. Through a simple lab survey consisting of 26 users, three important facts had been concluded: 1) personal privacy protection is still an important factor that influences the users to choose their smartphones; 2) although smartphone nowadays provides more functions protecting user privacy through complex user interface, people are not well adapted to those new functions; and 3) Sorting methods, as well as recommendation systems are still useful to assist users to protect their private data. The shortcomings of Zhou *et al.*'s study is that the number of participated user is relatively small. Moreover, there's no specific solution has been proposed to increase the users' awareness of privacy protection.

In summary, all the above mentioned works, which we list in Table 7, suggest that privacy leakage on some level is unavoidable for users to enjoy the sharing service. However, users' awareness of privacy leakage can be improved by listing threats from third-party websites/applications [132], [133], [136], [137], [140], recommending safe decisions to users [134], [139] and using cyber-technologies [89], [141], [142]. Although various techniques are proposed to raise the users' awareness level, most sharing service platforms only provide user agreement terms to warn about possible privacy leakage. There is still a large gap between forcing users to agree to terms, granting access permissions to sensitive data and motivating users to actively protect their own privacy. Platform and service providers should be encouraged to use the existing cyber-technology to maximize users' awareness of privacy issues. Future works and surveys can be conducted in this direction.

B. FROM THE PLATFORMS' PERSPECTIVE: PROTECTING SHARED INFORMATION

Although users can agree to share part of their personal information on the intermediate platform, the shared information/data still faces various potential attacks without proper regulation protocol setups or cyber technology implementations. Data analysis for different purposes exists in almost all third-party platforms [156]. The main purpose of data analysis is to achieve better service quality. However, privacy concerns make users reluctant to share sensitive information. In this section, several recent existing works for privacy protection from the platforms' perspective are surveyed.

Chen and Liu [148], Chen *et al.* [149], Chen and Guo [150] presented a random space encryption (RASP) scheme that produces secure privacy protection on the cloud. RASP provides service to transfer the analyzing data into an encrypted space with a two-stage encoding algorithm. The way of updating the encrypted database is another important challenge for their work.

Hong *et al.* [151] surveyed several existing privacy protection strategies under the distributed data sharing environment. The proposed privacy protection techniques were simultaneously applied to the database, queries or aggregation. The main insufficiency of their work is that they only focused on privacy-preserving schemes for time series data processing.

Dong *et al.* [152], [153] suggested a security policy based on existing encryption techniques. The proposed framework allows the users to dynamically access their own personal data freely. Both attribute based encryption (ABE) and identity based encryption(IBE) were used to minimize the key management overhead; however, the proposed method resulted in key escrow problems [157].

Following Dong *et al.*'s work, Han *et al.* [154] provided a promising solution for privacy-preserved data outsourcing under the cloud environment. They proposed an attribute-based encryption (ABE) based control scheme on two major problems for data accessing privacy protection on the cloud. However, the time complexities of both the encryption and decryption processes in the proposed method were not optimized for real-world applications.

Le *et al.* [155] assumed that there were pre-defined rule regulations in the data processing scenarios. An inconsistency checking and removing algorithm was designed to ensure the enforceability for multi-access to stored data in cloud servers. The main concern of their work is that the pre-defined regulations can be not applicable under extreme conditions or worst case scenarios.

Wang *et al.* [144]–[146], Liu *et al.* [147] sproposed a hierarchical encryption scheme to maintain access controls

TABLE 7. References, main objectives, proposed solutions and important insufficiency of the surveyed works for increasing privacy awareness.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Malandrino *et al.* [132], [133]	2011, 2013	Measuring revealed data by service provider and privacy leakage to third-party websites	'NoTrace' software	Lacking of analysis on necessary information disclosure for a known service
Omoronyia *et al.* [134]	2013	Assisting privacy disclosure decisions made by applications	An adaptive privacy framework	Lacking systematical privacy requirements listing for a given set of service functions
Amini *et al.* [136], [137]	2013, 2014	Helping users better understand the functionality of mobile applications	AppScanner	A detailed categorization according to the behaviors purposes can be more helpful
Zhu *et al.* [139]	2014	Recommending mobile apps to users with security and privacy awareness	A mobile app recommendation system	The security risks are only evaluated based on the permissions that the apps request
Hartmann *et al.* [140]	2016	Addressing threats of mobile apps and proposing solutions	Eight recommendations for six main threats	No immediate solution is provided
Chandramohan *et al.* [141]	2016	Protecting user privacy on cloud	Petri-net Privacy-Preserving Framework	The practicability and real-time applicability of their algorithm need further discussion
Quay-de la Vallee *et al.* [142]	2016	Managing apps's access permissions	Two management apps	The privacy management assistance was only provided after the apps been installed
Ismail *et al.* [89]	2015	Identifying the minimal number of permissions to keep the mobile apps fully functioning	A crowdsourcing strategy	The proposed strategy is only tested on one single mobile app
Zhou *et al.* [143]	2017	accessed the gap between users' desire of privacy control and the actual privacy setting functions provided by mobile app systems	A simple lab survey consisting of 26 users	No specific solution was proposed

for different levels of users (Figure 10). Each domain master generates keys to a specific group of users in the next sub-level. In addition, they also proposed a scalable revocation scheme for users to access their own personal data. The proposed scheme lacked user revocation and was only applicable to the situation that all attributes were administered by the same domain authority.

Rahman *et al.* [21] reviewed 139 works from 2009 to 2014 regarding information security in cloud computing. The cyber technology of incident handling strategy (IHS) is heavily discussed, which is an important tool for protecting data in a shared cloud service system. They pointed out that although IHS setup is straightforward on a personal computer, it becomes complicated when cloud computing allows multiple computers to access the same data on the same hard-disk. The main insufficiency of their work is that the survey was done in 2014 and only covered IHS techniques proposed before that year.

In summary, a list of the surveyed works can be found in Table 8. From the platforms' point of view, there are mainly two parts of the data sharing practice can be worked on to provide more secure sharing services: the data transmission process and the data storage on the cloud server. To protect sensitive data during the data transmission process, data encryption is usually utilized [152], [153]. For data protection on the cloud server, encryption scheme [148]–[150],

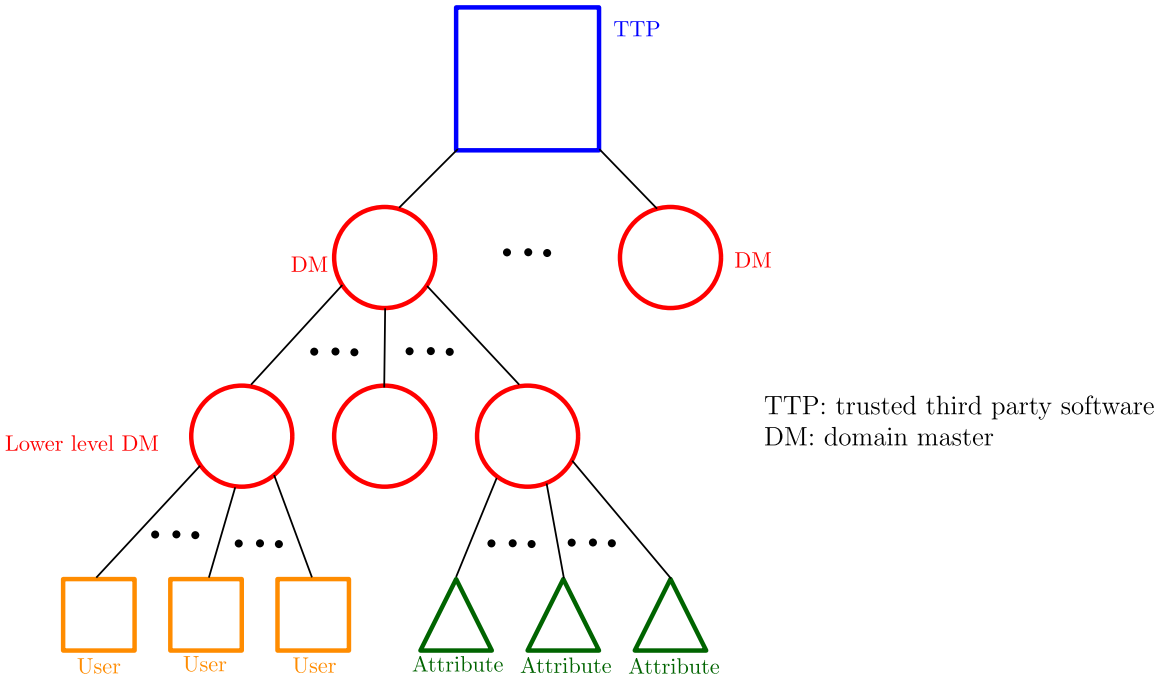

FIGURE 10. The hierarchical encryption scheme proposed by Wang *et al.* [144]–[147]: the trusted third party has the access control for the domain masters. The domain master generates keys to a specific group of users in the next sub-level. For example, the leftmost domain master acts like the office administrate who is in charge of all personnel in the office, but not to administer any other attributes.

a hierarchical data-accessing scheme [144], [154], [155], and other cyber technologies [21] were used. We believe that establishing an effective protocol in the platform is beneficial for both users and service providers. Although data analysis is necessary for service quality improvement, the part of the user data that must be revealed to the analyzer to obtain the full functionality of the sharing service remains questionable.

C. FROM THE SERVICE PROVIDERS' PERSPECTIVE: MAKING PRIVACY THE TOP PRIORITY

As the last but important participant, the service provider has to learn the importance of protecting user privacy. Numerous studies have shown that privacy protection/security level is an important component of the overall service quality, and therefore influences the final profit of the company [159], [162], [163]. More specifically, the enhancement of privacy protection quality by the service provider potentially attracts more customers to pay for the service [164]. Service providers must give the privacy protection issue the highest priority in a successful business model.

Thaichon *et al.* [159] surveyed the relationships between various aspects of service quality and the perceived value by customers. They identified the four most important service quality dimensions that influence the final profit of the company, which include privacy concerns. The limitation of their work is that the survey is conducted in the context of a single country (Thailand).

Hartono *et al.* [160] further identified the most important dimensions of perceived security for online purchases as confidentiality, integrity, availability, and non-repudiation. They validated that these four aspects significantly impact the customer's willingness to participate e-commerce services by using a second-order structural model of perceived security. In their experiment, only responses from Korea were used, which reduces the generalization of the study results.

Ingham *et al.* [161] examined the internal relationships among trust, perceived risks and customers' acceptance in e-shopping practices. The technology acceptance model (TAM) nomological network is deeply discussed to measure the values in a different dimensions. The testing results are analyzed by the meta-analytical path approach. This was a comprehensive survey paper that searched for potential ways to promote e-commerce to achieve better sales. However, regulation or cyber technology solutions for enhancing the trusts gained from the customers are missing.

Wang and Lin [158] established a conceptual research framework for studying the internal links between service quality and user experience of location-based services (LBS) (Figure 11). Based on a survey with 1399 participants, Wang and Lin identified positive and negative influences between factors, such as service quality and privacy trust in using LBS. Cultural bias exists in their results since the survey was conducted only in Taiwan.

All surveyed works from the service providers' perspective are listed in Table 9. The internal relationship between the

TABLE 8. References, main objectives, proposed solutions and important insufficiency of the surveyed works for protecting shared user data.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Chen *et al.* [148], [149], [150]	2005, 2011, 2013	Providing efficient and secure classifier using cloud computing technology with privacy preserved	A random space encryption (RASP) approach	Updating the encrypted database is not an easy task
Hong *et al.* [151]	2013	Preserving privacy under distributed environment	Surveying existing privacy protection strategies	Mainly focusing on time-series data mining
Dong *et al.* [152], [153]	2014, 2015	Suggesting a privacy-preserving data security policy	A series of encryption techniques	Resulting in key escrow problems
Han *et al.* [154]	2016	privacy-preserved data outsourcing under cloud environment	ABE based privacy protected data access control scheme	Requiring efficiency improvements
Le *et al.* [155]	2014	Ensuring the enforceability for multi-access to stored data in cloud servers	An inconsistency checking and removing algorithm	Requiring pre-defined rule regulations
Wang *et al.* [144], [145], [146], [147]	2011, 2013, 2014	Keeping the shared data confidential against untrusted cloud service providers	The hierarchical attribute-based encryption scheme	lacking user revocation and was restricted by the same domain condition
Rahman *et al.* [21]	2015	Protecting shared data on cloud	An information protection model combining incident handling strategy and digital forensics principles	The surveyed works were only up to the year 2014

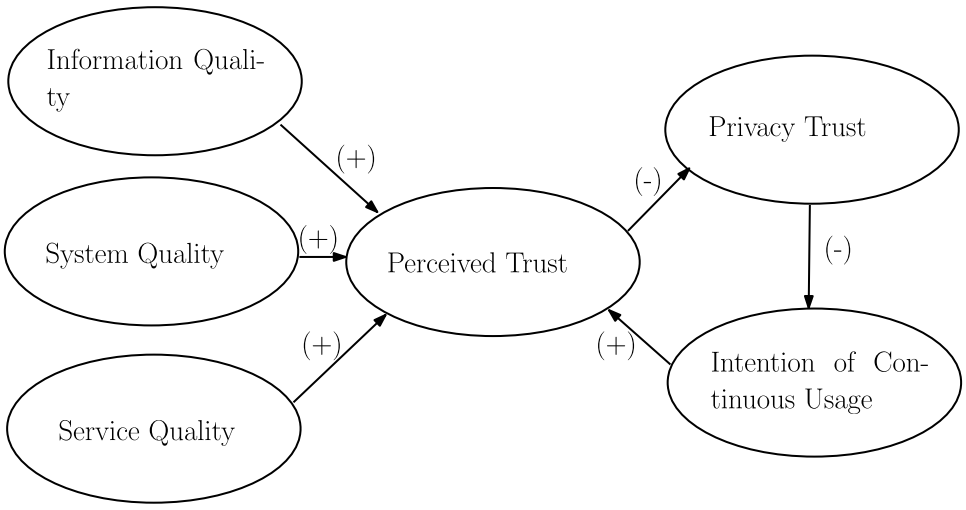

FIGURE 11. The research conceptual framework proposed by Wang and Lin's studies on the relationship between various elements on service quality and the intention of continuous usage of location based services [158]. The positive and negative influences between factors are marked by '+' and '−' signs.

privacy protection and the net profit is heavily studied. The privacy protection level is an essential component in service quality evaluation and significantly impacts the customers' willingness to participate, customers' trust and net profit. And certain degrees of privacy disclosure from the service providers' side can also increase the willingness of the customers to trust the sharing services. In conclusion, it is important for the service providers to consider privacy issues the top

TABLE 9. References, main objectives, proposed solutions and important insufficiency of the surveyed works for realizing the importance of protecting user privacy.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Thaichon *et al.* [159]	2014	determining the relation between different service quality aspects (including privacy protection) and the final profit	Identifying the four most important aspects for service quality enhancement	The survey results are only limited to a single country (i.e. Thailand)
Hartono *et al.* [160]	2014	Identifying the most important dimensions of perceived security for online shopping	A second-order structural model on perceived security	Only responses from Korea are used
Ingham *et al.* [161]	2015	Examining the internal relationship between trust, perceived risks, and customers' acceptance	The technology acceptance model (TAM) nomological network	Lacking ways to gain the customers' trusts
Wang and Lin [158]	2016	Studying the internal linking of service quality and intention of continuous usage of location-based services	A research conceptual framework	The survey was only conducted in Taiwan

priority of their commercial strategies, provide a more secure servicing environment and build more successful business models.

V. OPEN RESEARCH ISSUES

In the first part of this study, the cyber-enable sharing services are divided into six branches, which are crowdsourcing marketplace, crowdfunding, crowdtesting, collaborative online shopping, ridesharing and homesharing. In this section, we summarize the main open research issues from the above six branches and list them as follows:

1) **Improving task performance quality and efficiency with privacy-preserving protocols (crowdsourcing marketplace).** For Internet crowdsourcing marketplace, existing data manipulation approaches, such as coding theory and clipping protocols, decrease the task performance quality and efficiency. More efficient and effective mechanisms are demanded to better preserve the privacy from task requesters' perspective.
2) **Degree of privacy sacrifice for the requesters towards a successful crowdfunding campaign (crowdfunding).** Trust is the key component for a successful crowdfunding campaign [50], [59]. However, the most appropriate degree of privacy sacrifice for the requesters remains as an open problem to attract more funding contributions.
3) **Tradeoff between data encryption and testing result quality (crowdtesting).** Data encryption is a commonly used technique for protecting user privacy in crowdtesting practices, which unfortunately appear to decrease the testing result quality [165]. The way of balancing the tradeoff between data encryption and testing results quality is an important future working direction for crowdtesting practices.
4) **An integrated approach to prevent misuse of customers' data (collaborative online shopping).** Data misuse is the main threat for customers who participate in the collaborative online shopping practice. Although there are solutions from both regulation and technical side, an integrated approach is demanded to better protect the users' privacy.
5) **Conflict between location privacy and service based on location (ridesharing).** Location privacy is one of the hot topics in the field of location based services, such as ridesharing. However, there is always a conflict between hiding customers' real locations and utilizing the location information to serve customers better. A better solution to balance the conflict remains as an open problem in the field.
6) **Physical privacy protection for hosts (homesharing).** For homesharing practices, existing works focus on mechanisms of protecting customers' privacy. However, from our study, homesharing involves lots of interpersonal interactions, where the physical privacy violation is also a potential threat for the hosts. A well-regulated scheme to better protect the physical privacy for hosts involved in homesharing practices remains open.

In the second part of this work, the emerging privacy issues of the sharing services are further analyzed from three perspectives, namely, the users', platforms' and service providers' perspectives. The open problems from the three individual perspectives are:

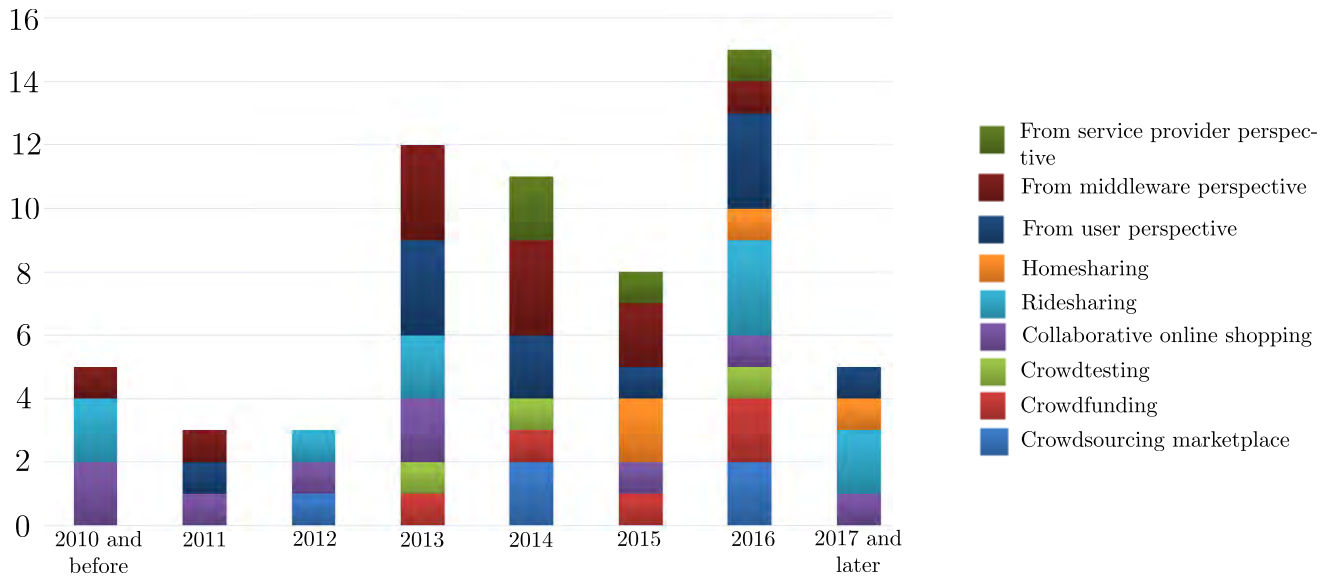

FIGURE 12. Yearly distribution of the number of all surveyed works from Table 1 to Table 9. Different colors are used indicating different types of sharing services.

- **From users' perspective: motivating users to protect their own privacy.** While most of surveyed works use cyber technologies to protect users from potential privacy leakage, we pointed out that those techniques can only be used against unnoticeable threats. Utilizing cyber techniques to motivate the users to actively protect their own privacy is still the main solution and must be further emphasized in future works.
- **From platforms' perspective: establishing effective protocol for data analysis.** Encryption is a mature and commonly used cyber technique to protect user information during the data transmission and storage in sharing service platforms. Our study shows that, on top of the data encryption, a more sophisticated protocol is demanded for platform companies to access the necessary data for analysis in order for them to provide better services.
- **From service providers' perspective: enhancing the awareness of the importance of privacy protection using cyber technology.** From service providers' perspective, the surveyed works indicated that the privacy protection level is directly co-related to the net profit. However, the way of enhancing service providers' awareness for the importance of protecting users' privacy using cyber technology remains as an open problem for future studies.

VI. CONCLUSIONS

Privacy issues will sooner or later become the main barriers for both users and service providers who participate in the sharing economy. Over the past few years, great research efforts have been devoted to address various privacy issues existed in sharing service practices. Figure 12 shows the yearly distribution of the number of all surveyed works from Table 1 to Table 9. Different colors are used to indicate various types of sharing services. It can be clearly seen that a substantial part of the works published in the recent five years, i.e., starting from 2013 to 2017 and later, is surveyed in this study.

The cyber-enabled sharing services were divided into two categories: crowdsourcing and collaborative consumption. Crowdsourcing is further divided into three branches: Internet crowdsourcing marketplace, crowdfunding and crowdtesting. In Internet crowdsourcing marketplace practices, we tackled the privacy protection problem for task requesters. Two approaches were surveyed: the coding theory and the instance clipping protocol. In crowdfunding practices, modern crowdfunding platforms, such as Indiegogo, allow users to select their preferred security level and conceal their personal information privately, such as their names and contribution amounts. However, the surveyed works suggest that a certain level of privacy sacrifice can be helpful in crowdfunding practice. For crowdtesting practices, three real-world applications were surveyed, including shared data protection on a the cloud server [55], online surveys [56] and indoor site survey practice [58]. The main difficulties in protecting the privacy in crowdtesting practices are identified, which leads to one of the future research directions in the crowdtesting field. In collaborative consumption, the three sub-categories are: collaborative online shopping, ridesharing and homesharing. Collaborative online shopping, as a new generation of online shopping experience, raises two potential privacy concerns. The first privacy concern is the misuse of user data for marketing analysis, which can be prevented by refining government regulation [76], masking customers' data before sending them out [85] or separating communication

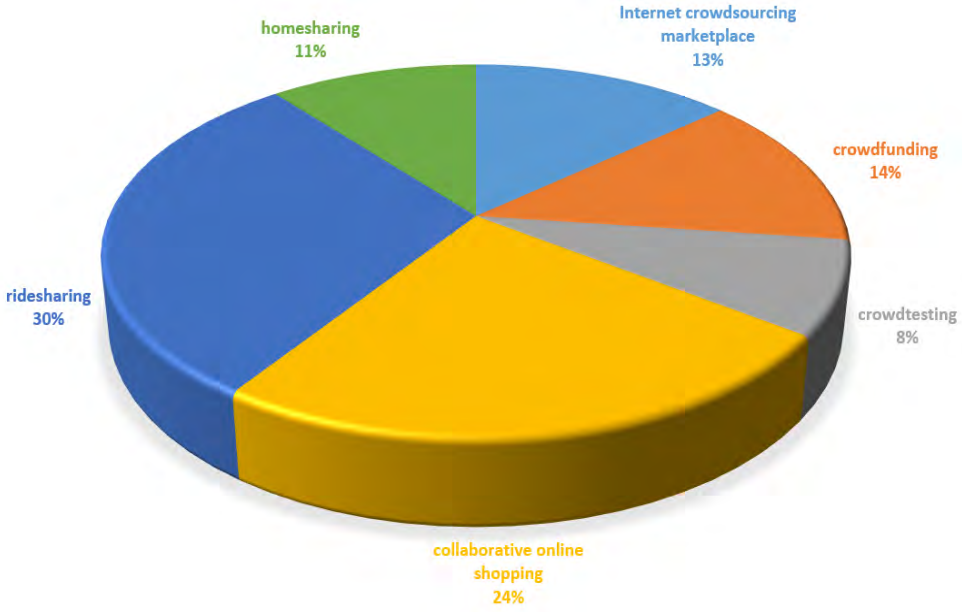

FIGURE 13. Statistical distribution of a total number of 37 works surveyed from Table 1 to Table 6.

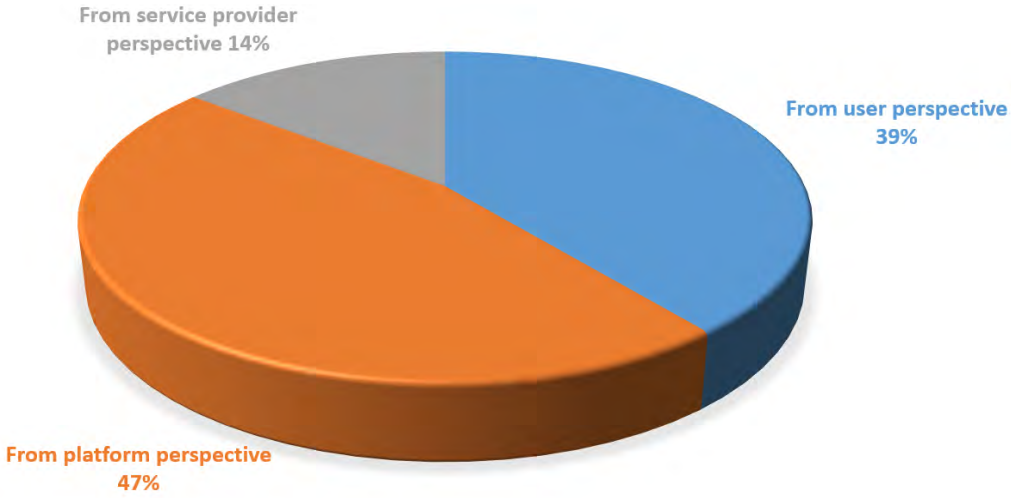

FIGURE 14. Statistical distribution of a total number of 28 works surveyed from Table 7 to Table 9.

channels on the cloud server [82]. The second privacy concern is related to users' awareness of privacy leakage in online shopping, which was further discussed in later sections. In ridesharing practice, it is important to note that revealing the passenger's information, such as location, is necessary for the user to utilize the service. For homesharing, the surveyed works reveal that the hosts are actually more concerned about their privacy leakage than the travellers. Most of the privacy concerns are physical privacy issues.

In summary, Figure 13 shows the distribution of all listed surveyed works from Table 1 to 6, including 37 works in total. In overall, the topics of privacy issues in collaborative online shopping and ridesharing are heavily discussed, whereas the topics of privacy issues in crowdtesting are less noticed. Although the surveyed works in this study do not include all works discussing the privacy issues of sharing services in the literature, the distribution reflects some aspects of the hotness/coldness of each mentioned topic, which provides potential directions to researchers for their future studies.

The above six branches of privacy concerns in the cyber-enabled sharing world are further summarized at the later part of this work from three perspectives. From the user perspective, users have started to realize that they have to sacrifice a certain degree of personal information to enjoy the sharing services. Therefore, the emerging issue is to increase the privacy awareness of the users. From the platform perspective,

TABLE 10. Important cyber techniques surveyed in this work: a technical comparison.

Method	Reference	Main technique	Advantage	Disadvantage
Coding theory	[29], [30], [31], [32]	Add random perturbations to sensitive data	Hide sensitive information from the workers	Lose the task performance quality
Instance clipping protocol (ICP)	[34], [35], [36]	Clip the task into pieces	Allow each work only to access one clipped piece	Decrease the quality of the task results
Collusion network	[37]	Integrate ICP with three operations	ICP with minimal privacy leakage (better than ICP)	Information leakage from the workers' side
SocialCrowd	[38]	Clustering algorithms with heuristic function	Data leakage was effectively prevented	High computational complexity
Encryption scheme for crowdtesting	[56], [58], [85]	Add noises to the test results	Sensitive data cannot be revealed easily	Original data can be distorted
π-box	[82]	Develop a third-party app to control sensitive data transmission	Separated channels are designed to control data transmission	Not all paid apps support π-box
Clustering k-anonymity (CK) scheme	[101], [102]	Encrypt the user location information	Help ridesharing companies in protecting the user location privacy	Decrease location information resolution; lack protection on sensitive data transmission
Anonymous mutual authentication (A-MA) protocol	[107], [108]	Develop AMA protocol for real-time navigation system	Conceal both customers and drivers' sensitive information (better than CK scheme)	A trusted third party middleware is required
Two-stage auction algorithm	[112]	Integrate k-anonymity scheme with ϵ-differential scheme	Conceal users' locations in a more sophisticated way	Add Gaussian white noise to actual locations
NoTrace	[132], [133]	Provide privacy recommendations to the users	Display the private information pieces received by service provider	Lack analysis on necessary information disclosure for a known service
AppScanner	[136], [137]	Let users better understand the functions of mobile apps	Provide informative description of what mobile apps do	Only categorize the mobile app behaviors as normal or abnormal
Mobile app recommendation systems	[139], [142]	Analyze security risks and request resource access permissions from users	More complete system design with detailed permission levels (better than NoTrace and AppScanner)	Security risks are hard to be measured during the installation process
Random space encryption (RASP) approach	[148], [149], [150]	Perform privacy protection on the cloud	Provide an encrypted space with a two-stage encoding algorithm on the cloud	Difficult to update an encrypted database
Attribute based encryption (ABE) scheme	[152], [153], [154]	Encrypt data on the cloud	Allow users to dynamically access personal data freely	Time complexities are not optimized for encryption and decryption processes
Hierarchical encryption scheme	[144], [145], [146], [147]	Maintain access controls for different levels of users	Each domain master generates keys to next sub-level users (better than ABE scheme)	Not applicable to the situations that attributes were administered by different domain authorities

it is necessary for the third party platform to analyze the user's shared data to improve the service quality. The emerging issue from the platform perspective is to develop an effective protocol for identifying and protecting sensitive data during the transmission process, as well as the storage on the cloud server. From the service provider perspective, privacy must be recognized as the most important issue in the business model, which potentially impacts the perceived security and trust as well as the final profit.

Figure 14 shows the distribution of all surveyed works from Table 7 to 9, including 28 works in total. In overall, most existing works focus on privacy protection solutions from user and platform perspectives. There are only a few works mentioning that the privacy protection level can be improved

by making the service providers realize the importance of protecting user privacy for their businesses. The privacy protection solution from the service providers' perspective deserves more attentions in future studies.

Table 10 covers the main cyber techniques surveyed in this work to protect privacy in sharing service practices. Each of these works was carefully evaluated to summarize its advantages/disadvantages compared with the remaining methods. All methods listed in Table 10 provide important solutions to protect privacy in different sharing service practices. Some of these methods can be more preferable under particular contexts or scenarios. For example, for privacy protection in crowdsourcing marketplace, SocialCrowd is preferred if the computational speed is not the main concern [38]. Otherwise, a collusion network, proposed by Celis *et al.* [37], can be more preferable to minimize the privacy leakage.

In conclusion, we would like to point out that the solutions for emerging privacy issues in the cyber-enabled world include many different aspects, such as developing a more sophisticated encryption scheme for masking the user data, proposing a more reliable recommendation system for user privacy management, implementing a more secure transmission protocol and etc. All these issues/solutions represent the future research directions for privacy protection in sharing service practices.

Conflict of Interests

All authors declare that there is no conflict of interest regarding the publication of this manuscript.

REFERENCES

[1] J. Ma, "Cybermatics for cyberization towards cyber-enabled hyper worlds," in *Proc. 4th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Mar./Apr. 2016, pp. 85–86.
[2] J. Ma *et al.*, "Perspectives on cyber science and technology for cyberization and cyber-enabled worlds," in *Proc. CyberSciTech (IEEE Cyber Sci. Technol. Congr.)*, Aug. 2016, pp. 1–9.
[3] J. Schor. (2014). Debating the Sharing Economy. Great Transition Initiative, Tellus Institute. [Online]. Available: http://www.greattransition.org
[4] G. Zervas, D. Proserpio, and J. W. Byers, "The rise of the sharing economy: Estimating the impact of airbnb on the hotel industry," *J. Marketing Res.*, vol. 54, no. 5, pp. 687–705, 2017.
[5] R. Belk, "You are what you can access: Sharing and collaborative consumption online," *J. Bus. Res.*, vol. 67, no. 8, pp. 1595–1600, 2014.
[6] G. Bella, R. Giustolisi, and S. Riccobene, "Enforcing privacy in e-commerce by balancing anonymity and trust," *Comput. Secur.*, vol. 30, no. 8, pp. 705–718, 2011.
[7] A. J. du Croix, "Data sharing and access protection in business system 12," *Comput. Secur.*, vol. 4, no. 4, pp. 317–323, 1985.
[8] N. Daswani, H. Garcia-Molina, and B. Yang, "Open problems in data-sharing peer-to-peer systems," in *Proc. Database Theory (ICDT)*. Berlin, Germany: Springer, 2003, pp. 1–15.
[9] M. Feeney. *Is Ridesharing Safe?* Accessed: Jan. 26, 2019. [Online]. Available: https://www.cato.org/publications/policy-analysis/ridesharing-safe?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed3A+PublicationsFromTheCatoInstitute+(Publications+from+the+Cato+Institute)
[10] M. M. Gobble, "Regulating innovation in the new economy," *Res.-Technol. Manage.*, vol. 58, no. 2, pp. 62–67, 2015.
[11] Y. Li, Y. Li, Q. Yan, and R. H. Deng, "Privacy leakage analysis in online social networks," *Comput. Secur.*, vol. 49, pp. 239–254, Mar. 2015.
[12] T. Dimitriou and A. Michalas, "Multi-party trust computation in decentralized environments," in *Proc. Int. Conf. New Technol., Mobility Secur.*, 2012, pp. 1–5.
[13] T. Dimitriou and A. Michalas, "Multi-party trust computation in decentralized environments in the presence of malicious adversaries," *Ad Hoc Netw.*, pp. 53–66, Apr. 2014.
[14] V. Katz, "Regulating the sharing economy," *Berkeley Technol. Law J.*, vol. 30, no. 4, p. 1067, 2015.
[15] D. Christin, "Privacy in mobile participatory sensing: Current trends and future challenges," *J. Syst. Softw.*, vol. 116, pp. 57–68, Jun. 2016.
[16] R. Botsman and R. Rogers, *What's Mine is Yours: How Collaborative Consumption is Changing the Way We Live*. London, U.K.: Collins, 2011.
[17] A. Doan, R. Ramakrishnan, and A. Y. Halevy, "Crowdsourcing systems on the World-Wide Web," *Commun. ACM*, vol. 54, no. 4, pp. 86–96, Apr. 2011.
[18] S. Androutsellis-Theotokis, "A survey of peer-to-peer file sharing technologies," 2002. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.12.8524
[19] C. C. Aggarwal and P. S. Yu, "A general survey of privacy-preserving data mining models and algorithms," in *Privacy-Preserving Data Mining*. Boston, MA, USA: Springer, 2008, pp. 11–52.
[20] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surv.*, vol. 42, no. 4, pp. 14-1–14-53, Jun. 2010.
[21] N. H. A. Rahman, and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *Comput. Secur.*, vol. 49, pp. 45–69, Mar. 2015.
[22] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Comput. Secur.*, vol. 53, pp. 1–17, Sep. 2015.
[23] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001.
[24] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
[25] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "ℓ-diversity: Privacy beyond k-anonymity," in *Proc. ACM Trans. Knowl. Discovery Data (TKDD)*, vol. 1, no. 1, 2007, p. 24.
[26] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and ℓ-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Apr. 2007, pp. 106–115.
[27] J. Howe, "The rise of crowdsourcing," *Wired Mag.*, vol. 14, no. 6, pp. 1–4, Jun. 2006.
[28] A. Kittur, E. H. Chi, and B. Suh, "Crowdsourcing user studies with mechanical turk," in *Proc. ACM SIGCHI Conf. Hum. Factors Comput. Syst.*, 2008, pp. 453–456.
[29] L. R. Varshney, "Privacy and reliability in crowdsourcing service delivery," in *Proc. IEEE Annu. SRII Global Conf.*, Jul. 2012, pp. 55–60.
[30] A. Vempaty, L. R. Varshney, and P. K. Varshney, "Reliable crowdsourcing for multi-class labeling using coding theory," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 667–679, Aug. 2014.
[31] A. Vempaty, Y. S. Han, L. R. Varshney, and P. K. Varshney, "Coding theory for reliable signal processing," in *Proc. IEEE Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2014, pp. 200–205.
[32] T.-Y. Wang, Y. S. Han, P. K. Varshney, and P.-N. Chen, "Distributed fault-tolerant classification in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 724–734, Apr. 2005.
[33] L. R. Varshney, A. Vempaty, and P. K. Varshney, "Assuring privacy and reliability in crowdsourcing with coding," in *Proc. IEEE Inf. Theory Appl. Workshop (ITA)*, Feb. 2014, pp. 1–6.
[34] G. Little and Y.-A. Sun, "Human OCR: Insights from a complex human computation process," in *Proc. Workshop Crowdsourcing Hum. Comput., Services, Stud. Platforms, ACM CHI*, 2011.
[35] K. Chen, A. Kannan, Y. Yano, J. M. Hellerstein, and T. S. Parikh, "Shreddr: Pipelined paper digitization for low-resource organizations," in *Proc. 2nd ACM Symp. Comput. Develop.*, 2012, p. 3.
[36] H. Kajino, Y. Baba, and H. Kashima, "Instance-privacy preserving crowdsourcing," in *Proc. 2nd AAAI Conf. Hum. Comput. Crowdsourcing*, 2014, pp. 96–103.
[37] L. E. Celis, S. P. Reddy, I. P. Singh, and S. Vaya, "Assignment techniques for crowdsourcing sensitive tasks," in *Proc. 19th ACM Conf. Comput.-Supported Cooperat. Work Social Comput.*, 2016, pp. 836–847.
[38] I. B. Amor, S. Benbernou, M. Ouziri, Z. Malik, and B. Medjahed, "Discovering best teams for data leak-aware crowdsourcing in social networks," *ACM Trans. Web*, vol. 10, no. 1, p. 2, 2016.

[39] P. Belleflamme, T. Lambert, and A. Schwienbacher, "Crowdfunding: Tapping the right crowd," *J. Bus. Venturing*, vol. 29, no. 5, pp. 585–609, 2014.

[40] E. Mollick, "The dynamics of crowdfunding: An exploratory study," *J. Bus. Venturing*, vol. 29, no. 1, pp. 1–16, 2014.

[41] V. Kuppuswamy and B. L. Bayus, "Crowdfunding creative ideas: The dynamics of project backers in kickstarter," Univ. North Carolina Kenan-Flagler, Chapel Hill, NC, USA, Res. Paper 15–2013, 2014.

[42] N. Baddour, "Indiegogo insight: Pitch videos power contributions: Increasing them 114%," Indiegogo (blog), Dec. 1, 2011. [Online]. Available: http://blog.indiegogo.com/2011/12/indiegogo-insight-pitch-videos-power-contributions.html

[43] C. S. Bradford, "The new federal crowdfunding exemption: Promise unfulfilled," *Securities Regulation Law J.*, vol. 40, no. 3, May 2012. [Online]. Available: https://ssrn.com/abstract=2066088

[44] G. Burtch, A. Ghose, and S. Wattal, "An empirical examination of users' information hiding in a crowdfunding context," in *Proc. 34th Int. Conf. Inf. Syst. (ICIS)*, 2013, pp. 343–361.

[45] J. Snyder, "Crowdfunding for medical care: Ethical issues in an emerging health care funding practice," *Hastings Center Rep.*, vol. 46, no. 6, pp. 36–42, 2016.

[46] G. Burtch, A. Ghose, and S. Wattal, "An experiment in crowdfunding: Assessing the role and impact of transaction-level information controls," Jan. 2014. in *Proc. 35th Int. Conf. Inf. Syst. Building Better World Through Inf. Syst. (ICIS)*, Jan. 2014

[47] G. Burtch, A. Ghose, and S. Wattal, "The hidden cost of accommodating crowdfunder privacy preferences: A randomized field experiment," *Manage. Sci.*, vol. 61, no. 5, pp. 949–962, 2015.

[48] H. Zheng, J.-L. Hung, Z. Qi, and B. Xu, "The role of trust management in reward-based crowdfunding," *Online Inf. Rev.*, vol. 40, no. 1, pp. 97–118, 2016.

[49] M. Kang, Y. Gao, T. Wang, and H. Zheng, "Understanding the determinants of funders' investment intentions on crowdfunding platforms: A trust-based perspective," *Ind. Manage. Data Syst.*, vol. 116, no. 8, pp. 1800–1819, 2016.

[50] W. Shen, J. W. Crandall, K. Yan, and C. V. Lopes, "Information design in crowdfunding under thresholding policies," in *Proc. 17th Int. Conf. Auto. Agents Multiagent Syst.*, 2018, pp. 1–10.

[51] T. Zhang, J. Gao, and J. Cheng, "Crowdsourced testing services for mobile apps," in *Proc. IEEE Symp. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2017, pp. 75–80.

[52] M. Vuković, "Crowdsourcing for enterprises," in *Proc. IEEE World Conf. Services-I*, 2009, pp. 686–692.

[53] L. M. Riungu, O. Taipale, and K. Smolander, "Research issues for software testing in the cloud," in *Proc. IEEE 2nd Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Nov./Dec. 2010, pp. 557–564.

[54] pybossa. (2015). *Pybossa*. [Online]. Available: https://pybossa.com

[55] H. Harkous, R. Rahman, and K. Aberer, "C3P: Context-aware crowdsourced cloud privacy," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.* Cham, Switzerland: Springer, 2014, pp. 102–122.

[56] T. Kandappu, V. Sivaraman, A. Friedman, and R. Boreli, "Exposing and mitigating privacy loss in crowdsourced survey platforms," in *Proc. ACM Workshop Student Workhop*, 2013, pp. 13–16.

[57] P. McDonald, M. Mohebbi, and B. Slatkin, "Comparing Google consumer surveys to existing probability and non-probability based Internet surveys," Google Inc., Mountain View, CA, USA, White Paper, 2012.

[58] S. Li, H. Li, and L. Sun, "Privacy-preserving crowdsourced site survey in wifi fingerprint-based localization," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 123, 2016.

[59] T.-P. Liang, S. P.-J. Wu, and C.-C. Huang, "Why funders invest in crowdfunding projects: Role of trust from the dual-process perspective," *Inf. Manage.*, vol. 56, no. 1, pp. 70–84, 2018.

[60] C. Graham and R. L. G. Payne, *Dynamic System Identification. Experiment Design and Data Analysis. Mathematics in Science and Engineering*, vol. 136. New York, NY, USA: Academic, 1977.

[61] Ö. Uzuner, Y. Luo, and P. Szolovits, "Evaluating the state-of-the-art in automatic de-identification," *J. Amer. Med. Informat. Assoc.*, vol. 14, no. 5, pp. 550–563, 2007.

[62] E. Gilbert, K. Evans, T. Clark, and K. Beck, "De-identification and linkage of data records," U.S. Patent 09 931 069, Aug. 15, 2001.

[63] K. El Emam *et al.*, "A globally optimal k-anonymity method for the de-identification of health data," *J. Amer. Med. Inf. Assoc.*, vol. 16, no. 5, pp. 670–682, 2009.

[64] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information," in *Proc. PODS*, vol. 98, 1998, p. 188.

[65] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proc. IEEE 21st Int. Conf. Data Eng. (ICDE)*, 2005, pp. 217–228.

[66] J. Hamari, M. Sjöklint, and A. Ukkonen, "The sharing economy: Why people participate in collaborative consumption," *J. Assoc. Inf. Sci. Technol.*, vol. 67, no. 9, pp. 2047–2059, 2015.

[67] A. Wright, "Controlling risks of e-commerce content," *Comput. Secur.*, vol. 20, no. 2, pp. 147–154, 2001.

[68] D. A. Light, "Sure, you can trust us," *MIT Sloan Manage. Rev.*, vol. 43, no. 1, p. 17, 2013.

[69] N. E. Bowie and K. Jamal, "Privacy rights on the Internet: Self-regulation or government regulation?" *Bus. Ethics Quart.*, vol. 16, no. 3, pp. 323–342, 2006.

[70] D. A. Valentine, "Privacy on the Internet: The evolving legal landscape," *Santa Clara Comput. High Technol. Law J.*, vol. 16, no. 2, pp. 401–417, 2000.

[71] A. D. Miyazaki and A. Fernandez, "Consumer perceptions of privacy and security risks for online shopping," *J. Consum. Affairs*, vol. 35, no. 1, pp. 27–44, 2001.

[72] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, 2004.

[73] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," *Inf. Syst. Res.*, vol. 22, no. 2, pp. 254–268, 2011.

[74] W.-L. Shiau and M. M. Luo, "Factors affecting online group buying intention and satisfaction: A social exchange theory perspective," *Comput. Hum. Behav.*, vol. 28, no. 6, pp. 2431–2444, 2012.

[75] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," *Comput. Hum. Behav.*, vol. 53, pp. 419–426, Dec. 2015.

[76] S. Preibusch, T. Peetz, G. Acar, and B. Berendt, "Shopping for privacy: Purchase details leaked to PayPal," *Electron. Commerce Res. Appl.*, vol. 15, pp. 52–64, Jan./Feb. 2016.

[77] Y. Poullet, "EU data protection policy. The Directive 95/46/EC: Ten years after," *Comput. Law Secur. Rev.*, vol. 22, no. 3, pp. 206–217, 2006.

[78] O. S. Kerr, "Internet surveillance law after the USA Patriot Act: The big brother that isn't," *Nw. UL Rev.*, vol. 97, p. 607, 2002. [Online]. Available: https://heinonline.org/HOL/LandingPage?handle=hein.journals/illlr97&div=20&id=&page=

[79] A. Macrina, "Accidental technologist: The Tor browser and intellectual freedom in the digital age," *Reference User Services Quart.*, vol. 54, no. 4, p. 17, 2015.

[80] R. W. Proctor and K.-P. L. Vu, "Designing Web sites and interfaces to optimize successful user interactions: Symposium overview," in *Proc. Symp. Hum. Interface*. Springer, 2011, pp. 62–65.

[81] C. Perera, R. Ranjan, and L. Wang, "End-to-end privacy for open big data markets," *IEEE Cloud Comput.*, vol. 2, no. 4, pp. 44–53, Apr. 2015.

[82] S. Lee, E. L. Wong, D. Goel, M. Dahlin, and V. Shmatikov, "πBox: A platform for privacy-preserving apps," in *Proc. NSDI*, 2013, pp. 501–514.

[83] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, pp. 122–134, Jan. 2017.

[84] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *J. Consum. Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[85] A. Bilge and H. Polat, "A comparison of clustering-based privacy-preserving collaborative filtering schemes," *Appl. Soft Comput.*, vol. 13, no. 5, pp. 2478–2489, 2013.

[86] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in *Proc. Conf. Hot Topics Cloud Comput.*, 2009, pp. 1–5.

[87] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 405–419, Jul./Sep. 2017.

[88] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in *Proc. Int. Workshop Secur. Cloud Comput.*, 2014, pp. 35–42.

[89] Q. Ismail, T. Ahmed, A. Kapadia, and M. K. Reiter, "Crowdsourced exploration of security configurations," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst.*, 2015, pp. 467–476.

[90] N. D. Chan and S. A. Shaheen, "Ridesharing in North America: Past, present, and future," *Transp. Rev.*, vol. 32, no. 1, pp. 93–112, 2012.
[91] N. A. H. Agatz, A. L. Erera, M. W. P. Savelsbergh, and X. Wang, "Dynamic ride-sharing: A simulation study in metro Atlanta," in *Proc. 19th Int. Symp. Transp. Traffic Theory*, vol. 45, no. 9, Nov. 2011, pp. 1450–1464.
[92] W. Shen and C. Lopes, "Managing autonomous mobility on demand systems for better passenger experience," in *Proc. Int. Conf. Principles Pract. Multi-Agent Syst.* Cham, Switzerland: Springer, 2015, pp. 20–35.
[93] W. Shen, C. V. Lopes, and J. W. Crandall, "An online mechanism for ridesharing in autonomous mobility-on-demand systems," in *Proc. 25th Int. Joint Conf. Artif. Intell.*, New York, NY, USA, 2016, pp. 475–481.
[94] W. Shen, A. Al Khemeiri, A. Almehrzi, W. Al Enezi, I. Rahwan, and J. W. Crandall, "Regulating highly automated robot ecologies: Insights from three user studies," in *Proc. ACM 5th Int. Conf. Hum.-Agent Interact. (HAI)*, 2017, pp. 111–120.
[95] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan./Mar. 2003.
[96] A. Mitrokotsa, C. Onete, and S. Vaudenay, "Location leakage in distance bounding: Why location privacy does not work," *Comput. Secur.*, vol. 45, pp. 199–209, Sep. 2014.
[97] S. F. Shahandashti, R. Safavi-Naini, and N. A. Safa, "Reconciling user privacy and implicit authentication for mobile devices," *Comput. Secur.*, vol. 53, pp. 215–233, Sep. 2015.
[98] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Secure Data Management*. Berlin, Germany: Springer, 2005, pp. 185–199.
[99] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: A study of users' privacy concerns," in *Proc. INTERACT*, vol. 3, 2003, pp. 702–712.
[100] H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy using dummies for location-based services," in *Proc. IEEE 21st Int. Conf. Data Eng. Workshops*, Apr. 2005, p. 1248.
[101] L. Yao, C. Lin, X. Kong, F. Xia, and G. Wu, "A clustering-based location privacy protection scheme for pervasive computing," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.* Washington, DC, USA: IEEE Computer Society, Dec. 2010, pp. 719–726.
[102] X. Pan and X. Meng, "Preserving location privacy without exact locations in mobile services," *Frontiers Comput. Sci.*, vol. 7, no. 3, pp. 317–340, 2013.
[103] X. Pan, W. Chen, L. Wu, C. Piao, and Z. Hu, "Protecting personalized privacy against sensitivity homogeneity attacks over road networks in mobile services," *Frontiers Comput. Sci.*, vol. 10, no. 2, pp. 370–386, 2016.
[104] P. Jagwani and S. Kaushik, "Defending location privacy using zero knowledge proof concept in location based services," in *Proc. IEEE 13th Int. Conf. Mobile Data Manage.*, Jul. 2012, pp. 368–371.
[105] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TrPF: A trajectory privacy-preserving framework for participatory sensing," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 874–887, Jun. 2013.
[106] A. Elbery, M. ElNainay, F. Chen, C.-T. Lu, and J. Kendall, "A carpooling recommendation system based on social VANET and geo-social data," in *Proc. 21st ACM SIGSPATIAL Int. Conf. Adv. Geograph. Inf. Syst.*, 2013, pp. 556–559.
[107] J. Ni, K. Zhang, X. Lin, H. Yang, and X. S. Shen, "AMA: Anonymous mutual authentication with traceability in carpooling systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
[108] J. Ni, X. Lin, K. Zhang, and X. Shen, "Privacy-preserving real-time navigation system using vehicular crowdsourcing," in *Proc. VTC*, 2016, pp. 1–6.
[109] U. M. Aïvodji, S. Gambs, M.-J. Huguet, and M.-O. Killijian, "Meeting points in ridesharing: A privacy-preserving approach," *Transp. Res. C, Emerg. Technol.*, vol. 72, pp. 239–253, Nov. 2016.
[110] R. Shokri, G. Theodorakopoulos, and C. Troncoso, "Privacy games along location traces: A game-theoretic framework for optimizing location privacy," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, p. 11, Feb. 2017.
[111] I. J. Vergara-Laurens, L. G. Jaimes, and M. A. Labrador, "Privacy-preserving mechanisms for crowdsensing: Survey and research challenges," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 855–869, Aug. 2017.
[112] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Comput. Netw.*, vol. 135, pp. 32–43, Apr. 2018.
[113] H. Vertommen, "The structure and conformity of meaning of interpersonal behaviors in different forms of relationships," *Psychol. Belgica*, vol. 20, no. 5, pp. 287–299, 1980.
[114] S. M. Andersen and S. Chen, "The relational self: An interpersonal social-cognitive theory," *Psychol. Rev.*, vol. 109, no. 4, p. 619, 2002.
[115] E.-J. Cho, "Interpersonal interaction for pleasurable service experience," in *Proc. ACM Conf. Designing Pleasurable Products Interfaces*, 2011, p. 68.
[116] R. W. Belk, "Possessions and the extended self," *J. Consum. Res.*, vol. 15, no. 2, pp. 139–168, 1988.
[117] R. Belk, "Sharing," *J. Consum. Res.*, vol. 36, no. 5, pp. 715–734, 2010.
[118] R. da Panda, S. Verma, and B. Mehta, "Emergence and acceptance of sharing economy in India: Understanding through the case of Airbnb," *Int. J. Online Marketing*, vol. 5, no. 3, pp. 1–17, 2015.
[119] V. Gaikar. *First eBay, Now AirBnB: The Rise of Peer to Peer Marketplaces*. Accessed: Jan. 26, 2019. [Online]. Available: https://www.tricksmachine.com/2013/05/ebay-airbnb-peer-to-peer-marketplaces.html
[120] J. Jefferson-Jones, "Airbnb and the housing segment of the modern 'sharing economy': Are short-term rental restrictions an unconstitutional taking?" *Hastings Constitutional Law Quart.*, vol. 42, no. 3, p. 557, 2014.
[121] P. Kamal and J. Q. Chen, "Trust in sharing economy," in *Proc. PACIS*, 2016. [Online]. Available: https://aisel.aisnet.org/pacis2016/109/
[122] C. Morosan and A. DeFranco, "Disclosing personal information via hotel apps: A privacy calculus perspective," *Int. J. Hospitality Manage.*, vol. 47, pp. 120–130, May 2015.
[123] E. Ert, A. Fleischer, and N. Magen, "Trust and reputation in the sharing economy: The role of personal photos in Airbnb," *Tourism Manage.*, vol. 55, pp. 62–73, Aug. 2016.
[124] M. Hoshmand. *The Risk of Being a Host in the Sharing Economy*. Accessed: Jan. 26, 2019. [Online]. Available: http://www.plaintiffmagazine.com/item/the-risks-of-being-a-host-in-the-sharing-economy
[125] C. Lutz, C. P. Hoffmann, E. Bucher, and C. Fieseler, "The role of privacy concerns in the sharing economy," *Inf. Commun. Soc.*, vol. 21, no. 10, pp. 1472–1492, 2017.
[126] S. J. Milberg, S. J. Burke, H. J. Smith, and E. A. Kallman, "Values, personal information privacy, and regulatory approaches," *Commun. ACM*, vol. 38, no. 12, pp. 65–74, 1995.
[127] X. Luo, "Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory," *Ind. Marketing Manage.*, vol. 31, no. 2, pp. 111–118, 2002.
[128] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, USA: Stanford Univ. Press, 2009.
[129] Y. Wang, Y. Huang, and C. Louis, "Respecting user privacy in mobile crowdsourcing," *Proc. Sci.*, vol. 2, no. 2, p. 50, 2013.
[130] H. To, G. Ghinita, and C. Shahabi, "A framework for protecting worker location privacy in spatial crowdsourcing," *Proc. VLDB Endowment*, vol. 7, no. 10, pp. 919–930, Jun. 2014.
[131] *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission, Washington, DC, USA, 2012.
[132] D. Malandrino and V. Scarano, "Supportive, comprehensive and improved privacy protection for Web browsing," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust (PASSAT), IEEE 3rd Int. Conf. Social Comput. (SocialCom)*, Oct. 2011, pp. 1173–1176.
[133] D. Malandrino, A. Petta, V. Scarano, L. Serra, R. Spinelli, and B. Krishnamurthy, "Privacy awareness about information leakage: Who knows what about me?" in *Proc. 12th ACM Workshop Workshop Privacy Electron. Soc.*, 2013, pp. 279–284.
[134] I. Omoronyia, L. Cavallaro, M. Salehie, L. Pasquale, and B. Nuseibeh, "Engineering adaptive privacy: on the role of privacy awareness requirements," in *Proc. Int. Conf. Softw. Eng.* Piscataway, NJ, USA: IEEE Press, May 2013, pp. 632–641.
[135] R. Meis and M. Heisel, "Computer-aided identification and validation of privacy requirements," *Information*, vol. 7, no. 2, p. 28, 2016.
[136] S. Amini, "Analyzing mobile app privacy using computation and crowdsourcing," Ph.D. dissertation, ProQuest Dissertations Publishing, Ann Arbor, MI, USA, 2014.
[137] S. Amini, J. Lin, J. I. Hong, J. Lindqvist, and J. Zhang, "Mobile application evaluation using automation and crowdsourcing," 2013. [Online]. Available: https://pdfs.semanticscholar.org/f2cf/29d79839db588d2651e8e27048df20e6a30f.pdf

[138] H. Wang, J. Hong, and Y. Guo, "Using text mining to infer the purpose of permission use in mobile apps," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2015, pp. 1107–1118.
[139] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2014, pp. 951–960.
[140] H. Hartmann, T. Wambach, M. Meffert, and R. Grimm, "A privacy aware mobile sensor application," Institut West, Fachbereich 4, Informatik, Univ. Koblenz Landau, Mainz, Germany, 2016. [Online]. Available: https://kola.opus.hbz-nrw.de/files/1317/A_Privacy_Aware_Mobile_Sensor_Application.pdf
[141] D. Chandramohan, T. Vengattaraman, D. Rajaguru, and P. Dhavachelvan, "A new privacy preserving technique for cloud service user endorsement using multi-agents," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 1, pp. 37–54, 2016.
[142] H. Quay-de la Vallee, P. Selby, and S. Krishnamurthi, "On a (per) mission: Building privacy into the app marketplace," in *Proc. 6th ACM Workshop Secur. Privacy Smartphones Mobile Devices*, 2016, pp. 63–72.
[143] Y. Zhou, M. Piekarska, A. Raake, T. Xu, X. Wu, and B. Dong, "Control yourself: On user control of privacy settings using personalization and privacy panel on smartphones," *Procedia Comput. Sci.*, vol. 109, pp. 100–107, May 2017.
[144] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Comput. Secur.*, vol. 30, no. 5, pp. 320–331, 2011.
[145] G. Wang, F. Yue, and Q. Liu, "A secure self-destructing scheme for electronic data," *J. Comput. Syst. Sci.*, vol. 79, no. 2, pp. 279–290, 2013.
[146] G. Wang, Q. Liu, Y. Xiang, and J. Chen, "Security from the transparent computing aspect," in *Proc. IEEE Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2014, pp. 216–220.
[147] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inf. Sci.*, vol. 258, pp. 355–370, Feb. 2014.
[148] K. Chen and L. Liu, "Privacy preserving data classification with rotation perturbation," in *Proc. 5th IEEE Int. Conf. Data Mining*, Nov. 2005, p. 4.
[149] K. Chen, R. Kavuluru, and S. Guo, "RASP: Efficient multidimensional range query on attack-resilient encrypted databases," in *Proc. 1st ACM Conf. Data Appl. Secur. Privacy*, 2011, pp. 249–260.
[150] K. Chen and S. Guo, "Privacy preserving data classification with rotation perturbation," in *Proc. IEEE 13th Int. Conf. Data Mining (ICDM)*, Nov. 2013, pp. 991–996.
[151] S.-K. Hong, K. Gurjar, H.-S. Kim, and Y.-S. Moon, "A survey on privacy preserving time series data mining," in *Proc. 3rd Int. Conf. Intell. Comput. Syst. ICICS*, 2013, pp. 44–48.
[152] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *Comput. Secur.*, vol. 42, pp. 151–164, May 2014.
[153] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, "SECO: Secure and scalable data collaboration services in cloud computing," *Comput. Secur.*, vol. 50, pp. 91–105, May 2015.
[154] K. Han, Q. Li, and Z. Deng, "Security and efficiency data sharing scheme for cloud storage," *Chaos, Solitons Fractals*, vol. 86, pp. 107–116, May 2016.
[155] M. Le, K. Kant, and S. Jajodia, "Consistency and enforcement of access rules in cooperative data sharing environment," *Comput. Secur.*, vol. 41, pp. 3–18, 2014.
[156] K. S. Reddy and M. Balaraju, "Comparative study on trustee of third party auditor to provide integrity and security in cloud computing," *Mater. Today Proc.*, vol. 5, no. 1, pp. 557–564, 2018.
[157] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–16, 2016.
[158] E. S.-T. Wang and R.-L. Lin, "Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention," *Behav. Inf. Technol.*, vol. 36, no. 1, pp. 1–9, 2016.
[159] P. Thaichon, A. Lobo, C. Prentice, and T. N. Quach, "The development of service quality dimensions for Internet service providers: Retaining customers of different usage patterns," *J. Retailing Consum. Services*, vol. 21, no. 6, pp. 1047–1058, 2014.
[160] E. Hartono, C. W. Holsapple, K.-Y. Kim, K.-S. Na, and J. T. Simpson, "Measuring perceived security in B2C electronic commerce website usage: A respecification and validation," *Decis. Support Syst.*, vol. 62, pp. 11–21, Jun. 2014.
[161] J. Ingham, J. Cadieux, and A. M. Berrada, "e-shopping acceptance: A qualitative and meta-analytic review," *Inf. Manage.*, vol. 52, no. 1, pp. 44–60, 2015.
[162] A.-S. Cases, C. Fournier, P.-L. Dubois, and J. F. Tanner, Jr., "Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes," *J. Bus. Res.*, vol. 63, nos. 9–10, pp. 993–999, 2010.
[163] Y. L. Zhao and C. A. Di Benedetto, "Designing service quality to survive: Empirical evidence from chinese new ventures," *J. Bus. Res.*, vol. 66, no. 8, pp. 1098–1107, 2013.
[164] J. C. Roca, J. J. García, and J. J. de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Inf. Manage. Comput. Secur.*, vol. 17, no. 2, pp. 96–113, 2009.
[165] F. R. A. Neto and C. A. S. Santos, "Understanding crowdsourcing projects: A systematic review of tendencies, workflow, and quality management," *Inf. Process. Manage.*, vol. 54, no. 4, pp. 490–506, 2018.

KE YAN (M'–) received the bachelor's and Ph.D. degrees from the National University of Singapore and the Ph.D. degree in computer science, in 2012. From 2013 to 2014, he was a Postdoctoral Researcher with the Masdar Institute of Science and Technology, Abu Dhabi, United Arab Emirates. He currently serves as an Associate Professor with China Jiliang University. His research interests include multi-agent system design, machine learning, energy management system design, computer vision, computer graphics, and bioinformatics. He is a member of IEEE.

WEN SHEN received the B.Eng. degree from the Masdar Institute of Science and Technology and the M.Sc. degree from Northwestern Polytechnical University. He is currently pursuing the Ph.D. degree with the Department of Informatics, University of California at Irvine, Irvine. His research interests include multi-agent systems, human–machine interaction, and game theory.

QUN JIN (SM'–) is currently a tenured Full Professor and the Chair of the Department of Human Informatics and Cognitive Sciences, Faculty of Human Sciences, Waseda University, Japan. He has been engaged extensively in research works in the fields of computer science, information systems, and social and human informatics. His research interests include human-centric ubiquitous computing, behavior and cognitive informatics, data analytics and big data security, personal analytics and individual modeling, cyber-enabled applications in e-learning and e-health, and computing for well-being. He is a Senior Member of IEEE and ACM.

HUIJUAN LU received the Ph.D. degree from the China University of Mining and Technology, in 2012. She is currently a Professor with China Jiliang University. Her current research interests include machine learning, pattern recognition, and bioinformatics. She is an Outstanding Member of the China Computer Federation.