A Survey on Security, Privacy, and Trust in Mobile Crowdsourcing

Wei Feng, Zheng Yan, *Senior Member, IEEE*, Hengrun Zhang, Kai Zeng, *Member, IEEE*, Yu Xiao, and Y. Thomas Hou, *Fellow, IEEE*

***Abstract*—With the popularity of sensor-rich mobile devices (e.g., smart phones and wearable devices), mobile crowdsourcing (MCS) has emerged as an effective method for data collection and processing. Compared with traditional wireless sensor networking, MCS holds many advantages such as mobility, scalability, cost-efficiency, and human intelligence. However, MCS still faces many challenges with regard to security, privacy, and trust. This paper provides a survey of these challenges and discusses potential solutions. We analyze the characteristics of MCS, identify its security threats, and outline essential requirements on a secure, privacy-preserving, and trustworthy MCS system. Further, we review existing solutions based on these requirements and compare their pros and cons. Finally, we point out open issues and propose some future research directions.**

***Index Terms*—Mobile crowdsourcing (MCS), privacy, security, trust, wireless sensor network (WSN).**

I. Introduction

WITH the rapid development of mobile and communication technologies, mobile and wearable devices have become an indispensable part of people's daily life. Nowadays, mobile devices are usually equipped with abundant sensors, which allows them to collect various types of data such as image/voice/video, location, and ambient information. The powerful computing capabilities that come with today's mobile devices allow them to perform many complex computing tasks, such as MapReduce-based parallel data processing. Moreover, advances of communication technologies such as 5G cellular networks, Wi-Fi, and Bluetooth, offer mobile devices direct connectivity to the Internet to exchange data at high speed at anytime and anywhere.

Mobile crowdsourcing (MCS) has emerged as a popular and effective method for data collection and data processing by utilizing the sensing, communication, and computing capabilities of the widely available mobile devices. It combines the concepts of crowdsourcing and mobility. An MCS system is open to mobile devices to participate in any sensing and computing tasks. It allows outsourcing a complex task that is usually difficult to be completed by a single computer or a group of people to an unspecified group of mobile devices. MCS that involves human intelligence, called human-assisted MCS, is an effective method to perform tasks that are easy for humans but remain difficult for machines. Human-assisted MCS can help build collaborative intelligence between human and machines.

In recent years, MCS has attracted much attention from both academia and industry. Many MCS applications have been developed [1]–[31] and are used for environment monitoring [2], [4], infrastructure monitoring [3], [10], [11], quality-of-experience analysis [8], [9], surface perception [5], and public safety [7]. In parallel to MCS applications, there are some studies aiming at improving the energy-efficiency in MCS [32], [33]. For instance, Lane *et al.* [33] proposed piggyback crowd sensing, which tried to reduce the overhead of data collection by exploiting Smartphone App opportunities.

MCS has a number of advantages over traditional wireless sensor networks (WSNs). First, MCS system saves the extra cost of installation and maintenance of new hardware infrastructure by leveraging the widely distributed mobile devices for data collection and processing. Therefore, its deployment and operation cost is lower than WSN. Second, the sensing devices in MCS are mobile and can provide a wider coverage than WSN. Third, MCS can perform instant data collection in a more flexible and cheaper way than WSNs. For example, in the application of urban traffic monitoring, it could be costly to deploy sensors that can cover a whole transportation network. This problem can be easily solved with MCS, due to the ubiquity of mobile devices. Fourth, MCS can be easily applied to sense big and temporary data. Massive data could be generated via MCS, thanks to the system scalability. For those tasks that need to collect data from a certain area just once, deploying sensors is costly and unnecessary. In contrast, MCS can conduct data collection in a convenient and

Manuscript received June 28, 2017; revised September 25, 2017; accepted October 7, 2017. Date of publication October 23, 2017; date of current version August 9, 2018. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800704, in part by the NSFC under Grant 61672410 and Grant U1536202, in part by a project through the Natural Science Basic Research Plan in Shaanxi Province, China, under Program 2016ZDJC-06, in part by the 111 Project under Grant B16037 and Grant B08038, and in part by the Academy of Finland under Grant 308087. The work of Y. T. Hou was supported by the U.S. National Science Foundation under Grant CNS-1443889, Grant CNS-1446478, and Grant CNS-1405747. *(Corresponding author: Zheng Yan.)*

W. Feng is with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: bjxsakya@qq.com).

Z. Yan is with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China, and also with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland (e-mail: zheng.yan@aalto.fi).

H. Zhang and K. Zeng are with the Department of Electrical and Computer Engineering, Department of Computer Science, and Center for Secure Information Systems, George Mason University, Fairfax, VA 22030 USA (e-mail: hzhang18@masonlive.gmu.edu; zengkai08@gmail.com).

Y. Xiao is with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland (e-mail: yu.xiao@aalto.fi).

Y. T. Hou is with the Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061 USA (e-mail: thou@vt.edu).

Digital Object Identifier 10.1109/JIOT.2017.2765699

self-organized manner in such scenarios. Finally, MCS provides a way to involve and utilize both human and machine intelligence.

In spite of the great benefits that MCS gains, it still faces a number of serious problems in terms of security, privacy, and trust. First, the nature of openness and mobility leads to the situation where it is easy to behave selfishly and raise attacks. This would cause serious security threats in MCS, such as eavesdropping and monitoring, collusion, tampered data uploading, and so on. Second, privacy is a crucial issue in MCS. The data collected via MCS may contain plenty of sensitive information about mobile users, which is directly related to user privacy. This gives chances for attackers to infer user private information from the collected data. For example, some MCS applications collect GPS fixes or cellular network IDs, from which a user's location and his/her physical activities can be inferred [114]. Besides, the privacy of an MCS service requestor may also be endangered because the task he/she requests may relate to some sensitive information. Third, data trust (DT) is a big issue in MCS. The openness of MCS offers almost all mobile users an opportunity to participate in MCS activities. As a result, the workers in MCS may be unreliable and vary in terms of ability, honesty, dependability, loyalty and so on. Accordingly, the data generated by different workers also vary in terms of trustworthiness that concerns data quality and reliability. If the above-mentioned security, privacy, and trust issues cannot be well solved, they may severely hinder the adoption of MCS applications.

In this paper, we review the existing studies in the area of MCS security, privacy, and trust by analyzing the characteristics of MCS, specifying its security threats, and then summarizing the requirements for achieving a secure, privacy-preserving and trustworthy MCS system. Furthermore, we use the proposed requirements as a measure to thoroughly review existing solutions in the literature in order to figure out open research issues and propose future research directions. Although there are already several surveys on the security, privacy, or trust in MCS [113]–[120], [123]. They mostly concentrate on a single aspect. None of them offers a comprehensive overview and analysis on the state-of-the-art solutions taking into account security, privacy, and trust at the same time. They mainly investigated technologies for solving security problems and discussed MCS challenges. Differently from the existing surveys, we comprehensively consider the security, privacy, and trust issues in MCS. We define security, privacy, and trust requirements, and use them to evaluate the existing solutions. In the sequel, we find several open issues and some future research directions for building up a secure, privacy-preserving, and trustworthy MCS system. Specifically, the contributions of this survey can be summarized as follows.

1) We analyze the specific characteristics of MCS, explore its potential threats in terms of security, privacy, and trust, and specify the requirements on a secure, privacy-preserving, and trustworthy MCS system.
2) We review the current literature about MCS security, privacy, and trust countermeasures by analyzing and comparing their advantages and disadvantages according to the proposed requirements.
3) We further figure out a number of open issues and propose some future research directions to motivate research on MCS security, privacy, and trust.

The rest of this paper is organized as follows. Section II briefly introduces the specific characteristics and system architecture of MCS. We compare MCS with WSN to give a deep insight into MCS. In Section III, we analyze potential threats in terms of security, privacy, and trust in MCS, and investigate the special requirements for building up a secure and trustworthy MCS system with required privacy preservation. In Section IV, we comprehensively review the state-of-the-art of countermeasures in MCS by applying the requirements as a measure to analyze their performance, effectiveness, and comprehensiveness. Furthermore, we discuss open issues and future research directions in Section V. Finally, the conclusion is presented in the last section.

II. Overview of MCS

A. Application Scenarios and User Cases

MCS can be applied into different application scenarios. Herein, we classify it into the following categories based on the properties of a crowdsourcing task and whether human assistance is needed.

1) Mobile Crowd Computing: Mobile crowd computing leverages spare computing power of mobile devices to complete a computing task. Nowadays, mobile devices are powerful in terms of computing capability and data transmission. Therefore, it is possible to outsource a computing task to mobile devices and collect their computing results via various networks.

2) Mobile Crowd Sensing: Mobile crowd sensing is the most popular MCS system. It utilizes mobile devices as sensors to collect information about environments, infrastructures, and mobile users. It is widely applied in personal data collection, e.g., personal health data, and in environment monitoring, e.g., noise, weather, and pollution.

3) Human-Assisted Crowdsourcing: Human-assisted crowdsourcing aims to utilize human intelligence to finish a certain task. A typical example is image annotation, in which mobile users help finish a labeling and classification task. It could well solve a problem that remains challenging for computers.

B. System Architecture of MCS

1) System Model: Generally, there are three main parties in an MCS system, namely MCS service provider (SP), end user, and MCS worker, as shown in Fig. 1.

a) MCS service provider: MCS SP could be played by an organization or a corporation that provides a platform for crowdsourcing. It accepts service requests from MCS end users, deals with the requests, selects proper MCS workers, and assigns relevant tasks to them. After receiving expected data or computing results from the workers, MCS SP would aggregate them and deliver a final result to the MCS end users. To build a practical MCS platform, the MCS SP needs a mechanism that guarantees the quality of data or computing results with a low cost. An MCS SP could be acted by a single or

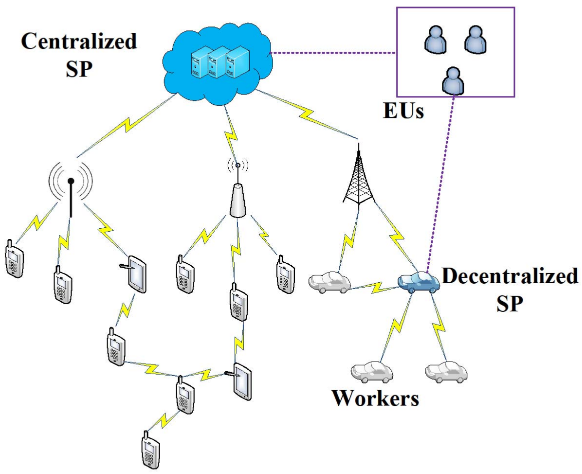


Fig. 1. System architecture of MCS.

a group of mobile users, who receive the task requests from the same or other mobile users and find a worker group to finish the task.

b) MCS end user: MCS end users are the users of MCS services. They request services offered by the MCS SP with a certain cost. An end user could be an individual or organization that lacks an ability to perform a certain computing or data collection task.

c) MCS worker: MCS workers are the mobile users who participate in crowdsourcing and perform the assigned tasks. There are mainly two kinds of workers, namely computing workers and sensing workers. The difference between them lies in the different tasks they perform. The computing workers act as computing nodes to perform computing tasks and upload their computing results to SP. SP normally aggregates and processes the computing results in order to provide a final result to end users. The sensing workers act as sensors to collect data.

Fig. 1 shows an architecture of MCS. Herein, we classify MCS into three categories according to their architecture, namely MCS with a centralized server, MCS with distributed servers, and fully distributed MCS. Generally, MCS is built with a centralized architecture, where SP is a server that collects data from workers and delivers data processing results to end users. This architecture usually suffers from single point failure or security attacks targeting at the central server. As a result, MCS with distributed servers was proposed [35], [36]. In [35], several decentralized servers cooperate to provide data storage or processing services. In the third category, fully distributed MCS, both SPs and workers are served by mobile devices. It is possible that a mobile end user directly requests data from other mobile devices without getting any SP involved.

2) Procedures of MCS Activities: To give an insight into how an MCS system works, we give a brief introduction to its workflow. First, an end user sends a request to an SP to initiate a task. After receiving the request, the SP analyzes the properties and requirements of the task. Based on the analysis, it divides the task into a number of subtasks, selects a dynamic group of mobile users as workers, and assigns the subtasks to them. The assignment of subtasks is determined by the requirements of the task. Worker selection and task allocation are based on the properties of workers, such as their abilities, locations, interests, etc. After receiving the assigned tasks, the workers perform the tasks and return their working results to the SP. The SP stores the received data or computing results, processes them and then presents the final results to the end user. Concerning the openness of MCS, there exist trust issues on both workers and data or computing results provided by them. Therefore, a trust management mechanism is usually needed in order to provide a reliable MCS service. From the above description, we can see that a practical and reliable MCS system should include the following procedures, as shown in Fig. 2.

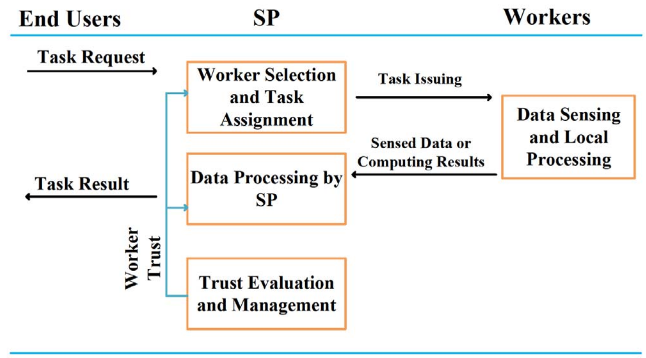


Fig. 2. MCS procedures.

1) *Worker Selection and Task Assignment:* This process selects a group of mobile users as workers and assigns the task to them. To provide a high-quality MCS service, it is important to guarantee the reliability and trustworthiness of workers. The requirements of a task should also be considered. Due to privacy and security concerns, or lack of interests, mobile users may be unwilling to participate in MCS activities. Therefore, an incentive mechanism is usually applied to attract more workers. In some designs, SPs encourage mobile users to serve as workers by offering them monetary rewards or extra services. A reasonable and effective worker selection and task assignment scheme should fulfill the following requirements. First, worker selection and task assignment should fulfill the requirements of the task, with regard to, for example, the number of workers and the coverage of their geo-locations. Second, the selection should guarantee high reliability, abilities, and trustworthiness of workers. Third, the worker selection process should ensure fairness. Both SP and workers should follow a predefined protocol and should not break their commitments. The SP should not forge selection results or the amount of payment, while the workers should not deny the workload they have committed to. Fourth, in this procedure, workers are probably required to upload some personal information, such as sensor types, computing capabilities, etc. The uploaded personal information should be carefully protected from being leaked to attackers. Fifth, the scheme could be able to resist several attacks, such as forging and collusion.

2) *Data Sensing and Processing by Workers:* In this step, MCS workers sense data or process data locally. In some cases, the workers are requested to perform some computing tasks. In other cases, the sensed data may contain redundant information that is not needed by a task. This not only generates extra computing and communication overhead, but also increases the possibility of privacy leakage. Therefore, even for data collection tasks, the data should also be processed locally to exclude redundant information to a certain extent, and to protect the private information that the data contains.
3) *Data Reporting:* In this procedure, the data generated by the workers is transmitted to the SP via various types of wireless networks. This procedure faces several challenges in security, privacy, and trust. The transmitted data may be highly related to the privacy of workers, and may suffer from several attacks such as eavesdropping and data tampering. Therefore, this process should guarantee the security and confidentiality of sensed data. SP should authenticate the provenance of data. The validity and the trust of data contributors should also be verified.
4) *Data Processing by SP and Presentation:* After receiving the reports from the workers, SP processes the data and finally generates the results according to the requirements of the end users. In most cases, SP is responsible for evaluating the quality of data generated by workers to ensure high quality-of-service. Since both SP and end users may be curious about workers' privacy, data processing should be performed in a privacy-preserving way. In addition, the final result presented to the end users should minimize the disclosure of worker privacy. Typical data processing in MCS includes truth discovery, quality evaluation, information fusion, data aggregation, data mining, etc.

Apart from the above four procedures, trust management is also an important part of the MCS system. Trust plays an important role in an MCS system, due to unevenness and unreliability of MCS parties. A trust mechanism measures the trust of mobile workers, and therefore is useful for worker selection and task assignment. In MCS, trust with impact of multiple factors (such as capability and honesty) should be considered. Therefore, it is necessary to measure the factors that influence trust, and to aggregate them to evaluate trust in a proper and accurate way.

C. Characteristics of MCS

MCS integrates the concepts of mobility with crowdsourcing. It is similar to WSN in the way that both of them can be applied for data collection. However, compared with WSN, MCS owns several special characteristics. In what follows, we summarize them and analyze MCS's differences from WSN.

1) MCS Versus WSN: Compared with WSN, the main difference is that MCS relies on mobile devices as sensors and utilizes existing communication networks for data collection and transmission. In this way, the deployment cost is pretty low. MCS is more flexible than WSN with regard to worker selection, because MCS can select any mobile devices in a sensing area based on the underlying requirements. However, this may result in involvement of distrusted mobile devices, and the data sensed is probably unreliable. Besides, how to encourage the participation of mobile users is also a practical problem in MCS. Specifically, MCS allows the involvement of human intelligence, which normally cannot be provided by WSN.

2) Special Characteristics: Based on the above description and analysis, we summarize the characteristics of MCS as below.

1) *Openness:* MCS is an open system that relies on the participation of mobile devices in data sensing or computing. Any mobile devices can participate as workers, and they do not need to belong to any MCS platform or owned by any SPs. Hence, malicious workers are not prevented from joining any MCS tasks. They may perform attacks to harm the privacy and security of SP, end users and other workers. Moreover, distrusted data or false data may be inserted by unreliable or malicious workers. As a result, it becomes essential to conduct accurate trust evaluation on workers and the collected data.
2) *Unreliability:* Unreliability is mainly caused by the openness of MCS. Workers differ from each other in terms of trust (e.g., ability, availability, reliability, and honesty). The unreliability may further result in the untrustworthiness of the collected data or the processing results. In addition, worker of low reliability is easier to be controlled by attackers, thus harming the whole MCS system.
3) *Mobility and Dynamic Topology:* The workers in MCS are mobile in nature. In a fully distributed MCS architecture, SP is also served by mobile devices. In this scenario, the topology of MCS becomes extremely complex. The mobility and dynamic topology makes worker management very challenging. Moreover, it also has a negative impact on key management in many cases. For example, in MCS-based cyber networking, frequent changes of base stations would cause changes of security parameters, such as keys and certificates.
4) *Network Heterogeneity:* Data in MCS can be uploaded to SP via various networks, such as 3G/4G/5G cellular networks, Wi-Fi, Bluetooth, and so on. Although this feature offers mobile devices multiple opportunities to connect to the SP in MCS, it also increases the risks of security, privacy, and trust. First, malicious nodes can perform several security attacks in certain kinds of networks. For example, it is easier to perform jamming attack in mobile ad-hoc networks (MANETs). Second, it increases difficulty in trust evaluation on data, since data transmitted through different networks suffers different interference. Therefore, they should be dealt separately when evaluating DT. Third, security protocols vary in different networks. It is necessary to solve the problems caused by different protocols when the underlying network changes.
5) *Data Massiveness and Diversity:* Compared with traditional online crowdsourcing and WSN, MCS can be

applied in various applications and scenarios. The popularity of mobile devices and network heterogeneity of MCS makes it possible to collect massive amount of data. The massiveness and diversity of data in MCS makes data processing more complicated in MCS than in other systems. It affects both DT and worker trust (WT). The massiveness and diversity increases the difficulty of data processing, and makes it hard to get accurate truth discovery result. As a result, the final result presented to end users may be deviated from the real truth. On the other hand, insufficient computing ability, data massiveness, and data diversity make it impossible to verify the accuracy of final results. Since WT is related to trust of the data he/she contributed, the hardness of accurate DT evaluation has a negative impact on WT evaluation. Besides, various data is likely to expose private information of workers, and thus harms the privacy of workers.

III. Requirements on Security, Privacy, and Trust

A. Concepts of Security, Privacy, and Trust

Security means protecting collected data and MCS systems from unauthorized access, use, disclosure, disruption, modification, destruction, etc. A secure MCS system should be able to resist security attacks, protect the collected data and processing results from leaking to unauthorized parties, and maintain the normal functions of the whole system.

However, it is not enough to guarantee the security of MCS only. Even if a system has proved to be secure, it may still leak some private information to others. For example, if an end user publishes his task without any protection, the privacy of end users may be harmed. Apart from security, a practical MCS system should also preserve the privacy of both end users and workers. Privacy usually means the ability of an entity to determine whether, when, and to whom the information about the entity is to be released or disclosed. Compared with security, privacy pays more attention to the protection of private information. Security helps improve privacy, but cannot guarantee privacy.

Trust can be seen as the confidence, belief, and expectation regarding the reliability, integrity, ability, and other characteristics of an entity [128]. In MCS, trust can be divided into WT, SP trust (ST), and collected DT. A worker with high trust should be of high computing and communication abilities, reliable, trustful and should behave honestly. High DT requires data to be accurate and trustworthy enough. Trust helps provide high-quality services and attract users.

B. Threat Analysis

As mentioned above, MCS faces serious problems in terms of security, privacy, and trust. All above issues relate to the three types of system parties in MCS, e.g., the privacy of both end users and workers. In what follows, we go through the main threats in terms of security, privacy, and trust in MCS.

1) Security Threats: Messages transmitted in MCS could contain sensitive information about end users and workers. Therefore, it is necessary to protect data or computing results from attackers or malicious parties. However, most devices in MCS are still constrained in terms of computing and communication capabilities. Besides, open wireless channel and distributed nature make it easy for attackers to perform eavesdropping and monitoring attacks. Even worse, as an open system, it is inevitable to include some selfish or malicious workers, which may perform various attacks and destroy the normal function of the system. Outsourcing a task to an unspecified or randomly generated group makes the management of workers very difficult. To better illustrate the security issues in MCS, we summarize potential security attacks in MCS and list them in Table I.

2) Privacy Threats:

a) Threats to data privacy of workers: The privacy issues concerning the workers are serious. One basic issue is sensed data privacy. MCS can be used to collect knowledge and environmental information surrounding workers as well as the information about their physical and social activities. Obviously, the data sensed by the workers probably contains private information. The exposure of these data would certainly harm the privacy of the workers. Some collected information, such as heartbeat rates and fingerprints, is related to the workers' privacy directly. Apart from sensed data privacy, some environmental information sensed by the workers can be utilized to infer extra information about their preference. For example, the pictures and audio samples may include unique features, which may reveal fine-grained details about the workers, such as user trajectory and preference. Another typical example is to obtain personal information from imaging data directly or through further inference, since images usually contains most sensitive information about participants, such as their appearance, location, and environment. Notably, the data privacy can be threatened in many ways. In MCS, data are first sensed by workers and transmitted to SP. The SP would store and process the data and then present the final results to the end users. The wireless communication channel makes it easy for the adversaries to monitor or eavesdrop the transmitted data. Illegal access to the collected or processed data at the SP may also harm data privacy.

b) Threats to personal information privacy of workers: Another privacy issue is about the personal information privacy of workers. Herein, personal information means the information about location, workload, computing ability and communication capacity, etc. that is uploaded to SP in the worker selection procedure, which is requested by SP for selecting proper workers. Personal information privacy requires protecting the uploaded information from leakage.

c) Threats to task privacy of end users: The privacy of an MCS service requestor may also be endangered because the task he/she requests may reveal some sensitive information. For the end users, the privacy issues are mainly caused by the potential privacy leakage from their task descriptions. The attackers can utilize the task information to deduce valuable information about the end users. Notably, outsourcing a task to a dynamic group of workers without effective protection could greatly impact the privacy of the end users. For example, if an end user publishes crowdsourcing tasks that can only be

TABLE I
POTENTIAL SECURITY ATTACKS IN MCS

Potential Attacks	Description
Eavesdropping.	The unauthorized real-time interception of messages that should be transmitted confidentially, such as collected data, personal information, etc.
Free Riding Attack	The free riding attack refers to that a worker receives a payment but devotes no effort to the completion of a task.
Sybil Attack	A malicious worker may launch multiple identities and then perform attacks, such as uploading false data to interfere the judgement of SP.
False Data Uploading	A worker uploads outdated, tampered or even fake data to SP.
Tracking	An attacker collects location based reports of workers and tries to decide their precise locations or trajectories.
False Personal Information Uploading	In the process of worker selection and task assignment, a mobile user uploads false information with regard to ability and resources, etc., intending to be selected as a worker.
Impersonation Attack	A malicious worker pretends to be another valid worker to upload false data or perform other misbehaviors.
Worker Selection Forging	SP breaks its commitment and falsely selects workers by disobeying a predefined protocol.
Worker Reward Forging	SP breaks its commitment and falsely determines the amount of reward for a selected worker.
DoS/DDoS Attack	DoS attack is a kind of attacks that harm the availability or dependability of a MCS service. If it is performed in a distributed way, it is DDoS attack.
Collusion	One party in MCS colludes with another one to pursue their own benefits or to achieve a certain goal. In MCS, there are mainly three kinds of collusion: 1. SP colludes with end users to determine a low reward for workers; 2. SP colludes with workers to generate a result with low quality for end users, or to forge worker selection results and worker rewards in order to reduce its cost; 3. Workers collude with each other to generate false data or repeated data.

fulfilled by psychologists, SP may infer that this end user may suffer from some psychological diseases. Therefore, the MCS system should guarantee identity privacy and task privacy for end users.

3) Trust Threats: MCS faces trust threats in terms of WT and DT, as well as ST. The WT threat is mainly caused by the intrinsic openness of MCS. Some workers may behave selfishly or maliciously and raise attacks by considering their own profits. Due to openness, workers in MCS usually vary in computing abilities, communication capacities, sensor types and reliability, etc. Lowly trusted workers, poor reliability, low computation capability, and a poor communication environment could negatively impact the quality of collected data and result in low DT. Therefore, the threats caused by both WT and DT should be paid attention to. ST is another important issue. In the centralized server architecture, ST is similar to cloud computing trust. In terms of a distributed server architecture or a fully distributed architecture, ST becomes a more challenging issue due to the nature of mobility, dynamicity and ubiquity of mobile SP in MCS.

In Table II, we summarize the potential attacks and the threats to security, privacy, and trust in MCS based on its working procedures to conclude the above analysis.

C. Requirements

Driven by the above threats analysis, we propose a number of requirements with regard to the security, privacy, and trust of an MCS system for the purpose of overcoming the potential attacks and security threats.

1) *Confidentiality and Integrity (C/I):* C/I are two basic properties that a secure system should fulfill. In a secure MCS system, collected data, computing results, task information, and personal information should all be protected from eavesdropping, modification, and leakage. The illegal reuse of historical data as up-to-date one should also be prevented. In MCS, the messages are transmitted via wireless channels, which are easy to be eavesdropped by attackers. Therefore, it is necessary to guarantee data C/I to resist eavesdropping attack and protect data from being tampered.
2) *Authenticity (Au):* Au is a key to resisting many identity-based attacks, such as Sybil and impersonation attacks. The MCS system should be able to verify that the data reports are from a valid worker that the sender declares. To provide Au, both provenance authentication and identity authentication should be offered. As an open system, MCS allows all kinds of mobile devices to participate in. Hence, there may exist selfish and even malicious workers or end users. Authentication helps exclude invalid and distrusted workers from a certain task, and guarantees that the data are generated from a preselected worker group, which helps improving data quality. Authentication on end users can deny some malicious tasks requested by attackers.
3) *WT:* WT represents the confidence on a worker with regard to its dependability, abilities (computing abilities, communication abilities, sensor abundance, etc.), reliability, worker preference, worker expertise, and availability of sensors, reputation, worker honesty, and loyalty. We expect that the workers selected for a task should be of high trust. In MCS, trusted workers should not only perform honest behaviors, but also fulfill the requirements of a certain task with high quality. To accurately evaluate a worker's trust, many influencing factors, such as worker dependability, reliability,

TABLE II
ATTACKS AND THREATS IN EACH PROCEDURE OF MCS

Procedures	**Attacks and Threats**		
	Security Related	**Privacy Related**	**Trust Related**
Worker Selection and Task Assignment	False Personal Information Uploading; Sybil Attack; Worker Selection Forging	Threat to Personal Information Privacy; Threat to Task Information Privacy	Threat to Worker Trust Threat to SP Trust
Data Sensing and Processing by Worker	Free Ridding Attack;	Threat to Personal Information Privacy; Threat to Data Privacy	Threat to Worker Trust Threat to Data Trust
Data Reporting	False Data Reporting; Sybil Attack; Tracking; Impersonation Attack	Threat to Personal Information Privacy; Threat to Data Privacy	Threat to Worker Trust Threat to Data Trust
Data Processing by SP	Various Attacks on a Single System Party (DoS/DDoS)	Threat to Personal Information Privacy; Threat to Data Privacy	Threat to Worker Trust Threat to Data Trust Threat to SP Trust
Trust Evaluation and Management	Impersonation Attack; False Personal Information Uploading; Sybil Attack	Threat to Personal Information Privacy; Threat to Data Privacy	Threat to Worker Trust Threat to Data Trust Threat to SP Trust

and worker abilities should be holistically considered. WT authentication can greatly help identifying selfish or malicious workers and thus support high quality MCS services.

4) *ST:* In MCS, SP is expected to be trusted and to perform its duties honestly. SP should select workers and calculate the reward for workers according to predefined protocols. On the other hand, the processing on the data collected from workers should be of high trust and the final result provided to end users should be of high quality. It requires that SP does not forge worker selection result, worker result or final results to obtain benefits.
5) *DT:* DT means that an MCS system should have the ability to figure out whether the collected data or computing results are trustworthy and the data with low trust is excluded. SP should also be able to deal with the data with low reliability so that the final result presented to end users is reliable and trustworthy. As aforementioned, sensed data in MCS varies in reliability, and cloaked or fake data may be generated by selfish or malicious workers. This requirement is important to deal with the data with low reliability and helps providing sound MCS services.
6) *Personal Information Trust (PT):* Personal information is usually requested by SP for worker selection. In reward-based worker selection and task assignment schemes, it influences the reward amount of a worker. Therefore, workers have incentive to upload false information to get more benefits. Therefore, PT should be ensured to block false personal information uploading, and to encourage workers to upload real information.
7) *Privacy (Pr):* Privacy requires that private information should not be leaked. In MCS, the privacy of both workers and end users should be considered. In MCS, the privacy includes the following three aspects: a) task privacy of end users; b) personal information privacy of end users and workers; and c) privacy of the collected data. Moreover, the privacy of the worker's identity is also very important. Identity information is directly related to the worker privacy. The data collected by the workers or its type can be used to infer sensitive information about them. The privacy of workers can be divided into data privacy, identity privacy, and personal information privacy. Most MCS services gather data around mobile workers themselves, which may reveal information sensitive to their privacy. Adversaries can extract personal information about workers, such as location information, trajectory, and preference by analyzing the data. Though data privacy is the most important part of privacy, the privacy of personal information that is requested in worker selection and task assignment (i.e., tasking) is also important and should be preserved. Another privacy issue in MCS is about the privacy of end users. The task information specified by the end users is probably related to their privacy. To support this requirement, the messages transmitted in the network should be protected to resist leakage of private information or data.
8) *Availability and Dependability (A/D):* A/D ensure survivability of MCS services to end users. The MCS services should be available even under denial-of-service (DoS) or distributed DoS (DDoS) attacks or in a poor communication environment. However, compared with traditional networks, MCS service should also be of high quality to well support A/D. That is, the final results presented to end users should be reliable enough. Both intermittent availability of MCS services and low-quality final output provided by a certain MCS SP may irritate end user experiences and thus hinder MCS adoption in practice.
9) *Nonrepudiation:* Usually, nonrepudiation (Nr) means that no party can deny the message it has sent. In MCS, for a worker, it means that the worker cannot deny the data it has provided and it should not deny the commitment to the task it has promised to perform. In terms of MCS SP, Nr means that it cannot deny the payment it has promised to offer to the worker. For an end user, it should also not be able to deny the task it has issued to SP. Nr can benefit to resist impersonate attack

TABLE III
REQUIREMENTS ON SECURITY, PRIVACY, AND TRUST IN MCS

	Security Level	Definition	Target Threats and Attacks
C/I	--	Any transmitted messages should be protected from eavesdropping and tampering.	Threat to Data Privacy; Threat to Personal Information Privacy; Threat to Task Information Privacy; Eavesdropping.
Au	--	The identity or validity of a message sender should be authenticated.	Threat to Worker Trust; Sybil Attack; Free Riding Attack; Impersonation Attack; DoS/DDoS Attack.
ST	High (H)	The scheme can detect or resist misbehaviors of SP, e.g., worker selection forging, and can resist all kinds of collusions.	Threat to SP Trust; Worker Selection Forging; Worker Result Forging; Collusion.
	Medium (M)	The scheme can detect or resist misbehaviors of SP, and can only resist some kinds of collusions listed in Table 1.	Threat to SP Trust; Worker Selection Forging; Worker Result Forging; Collusion.
	Low (L)	The scheme can detect or resist the misbehavior of SP, but fails to resist collusion attacks.	Threat to SP Trust; Worker Selection Forging; Worker Result Forging.
WT	High (H)	The worker trust is evaluated by comprehensively considering most of trust impact factors, such as worker ability (including reliability, computing capacity, etc.), sensed data trust, historical behavior trust, user preference, etc.	Threat to Data Trust; Threat to Worker Trust; Collusion.
	Medium (M)	One or two influencing factors are considered.	Threat to Data Trust; Threat to Worker Trust.
	Low (L)	Only part of a single factor influencing worker trust is considered.	Threat to Data Trust; Threat to Worker Trust.
DT	High (H)	The scheme considers most of the factors that influence data trust, such as network reliability, worker trust, worker ability, etc., and can resist false data uploading.	Threat to Data Trust; Threat to Worker Trust; False Data Uploading.
	Medium (M)	The scheme considers most of the factors influencing data trust, but cannot resist false data uploading.	Threat to Data Trust; Threat to Worker Trust.
	Low (L)	Data trust is guaranteed by providing user trust, and only part of trust influencing factors are considered.	Threat to Data Trust; Threat to Worker Trust.
PT	--	Personal information trust should be provided by discouraging false personal information uploading and encouraging workers to upload real information.	False Personal Information Uploading;
Pr	Personal Information Privacy (PP)	The privacy concerns personal information in the process of task assignment.	Threat to Personal Information Privacy; Tracking; Eavesdropping.
	Data Privacy (DP)	The privacy concerns data sensed or computed.	Threat to Data Privacy; Tracking; Eavesdropping.
	Task Privacy (TP)	The privacy concerns the task information related to end users.	Threat to Task Privacy; Eavesdropping.
	Identity Privacy (IP)	The privacy concerns the identity information of workers.	Threat to Personal Information Privacy; Eavesdropping.
A/D	--	The system could survive when being attacked or in a poor environment.	Threat to Data Trust; Threat to SP Trust; Threat to Worker Trust;

(Continued)

and the threats related to data transmission security, and help in maintaining the normal functions of the MCS system.

10) *Revocation:* Any workers or users should be excluded from MCS in time if they are detected as malicious, ineligible, harmful or invalid. This could help resisting

TABLE III (Continued)
REQUIREMENTS ON SECURITY, PRIVACY, AND TRUST IN MCS

Nr	--	Neither SP, end users, nor workers can deny the message that has been sent by them and the commitment they have promised.	Threat to SP Trust; Threat to Worker Trust; False Data Uploading; False Personal Information Uploading; Worker Selection Forging.
Re	--	Malicious or distrusted system parties should be excluded from the MCS system.	Threat to SP Trust; Threat to Worker Trust; Threat to Data Trust;
V	Selection Result Verification (SV)	The worker selection results can be verified to guarantee the fairness and correctness of selection.	Threat to SP Trust; Worker Selection Forging; Collusion.
	Processing Result Verification (PV)	The processing results performed by SP can be verified with regard to its quality and correctness.	Threat to SP Trust; Collusion.
	Reward Issuing Verification (RV)	SP should follow a pre-defined protocol to determine the reward for each worker, which can be verified by workers in some way.	Threat to SP Trust; Worker Reward Forging; Collusion.
AC	--	Only eligible parities that satisfy certain requirements can access collected data, uploaded worker personal information, task information or data processing results.	Threat to Data Privacy; Threat to Personal Information Privacy; Threat to Task Privacy.

DoS/DDoS attacks by preventing invalid mobile users from participating in MCS activities. Besides, it also helps improving the efficiency of worker selection due to the fact that only trusted workers should be involved into task fulfillment.

11) *Verifiability (V):* Verifiability means that the worker selection result, the issued rewards and the final results presented to end users can be verified in some way by workers or end users or public. That is, selection result verification (SV), processing result verification (PV), and reward issuing verification (RV) should be considered in MCS. On one hand, a method should be offered to end users to verify the correctness or evaluate the quality of the final results. On the other hand, in the process of task assignment, workers should be able to verify worker selection is fair and rewards are issued in a predefined and agreed way. Verifiability helps judging whether SP obeys the predefined protocols and checking the correctness of final crowdsourcing results.
12) *Access Control (AC):* For end users, they usually hope that the task information is only disclosed to valid workers, since it contains their sensitive information. Although workers agree to upload sensed data to SP, they may not be willing to disclose these data to others. Therefore, SP should deny any illegal access to the sensed data. A fine-grained AC mechanism can well solve this problem by allowing valid devices to access relative data based on the access policy defined by end users and workers.

The above requirements can be applied to evaluate the performance of existing schemes. For better evaluation, we further divide some of them into three levels, namely high, medium, and low, to measure how well an existing scheme fulfills each requirement. The detailed descriptions of requirements are given in Table III with our comments on why such requirements are proposed for overcoming which threats or attacks (i.e., target threats or attacks).

IV. COUNTERMEASURES

Although MCS brings great benefits, it still faces many problems in terms of security, privacy, and trust. Nowadays, much attention has been paid to building a secure, privacy-preserving, and trustworthy MCS system. In order to have a holistic understanding of the state-of-the-art, we review the related studies published in recent decade. We searched the databases: IEEE Explorer, ACM library, Springer library, and Elsevier library with the following keywords: security, privacy, trust, authentication, trust management, reputation, data aggregation, data processing, truth discovery, AC, and MCS/mobile crowd sensing/participatory sensing. We review the existing work by classifying them into six categories, i.e., secure worker selection and task assignment, secure data aggregation, truth discovery, trust management, AC, and secure and privacy-preserving data reporting. We examine whether each work fulfills the aforementioned requirements. For easy presentation and reading, we summarize all the abbreviations appeared in the rest of paper in Table IV with corresponding full terms. Table V summarizes our evaluation and comparison results with regard to the requirements specified in Section III.

A. *Secure Worker Selection and Task Assignment*

The procedure of worker selection and task assignment is responsible for dividing a requested task into subtasks, selecting a dynamic group of workers, and assigning the subtasks to them. Obviously, one main purpose of this procedure is to provide high-level WT, which means that the selected workers should be highly trusted. However, the trust of workers is determined by many factors, such as computing and communication abilities of workers, network reliability, worker

TABLE IV
ABBREVIATIONS

Abbreviation	Full Term
MCS	Mobile Crowdsourcing
WSN	Wireless Sensor Networking
PCS	Piggyback Crowd Sensing
SP	Service Provider
DoS	Denial of Service
DDoS	Distributed Denial of Service
AI	Auction Issuer
TLC	Time-Lapse Cryptography Service
TPK	Time-Lapse Public Key
TSK	Time-Lapse Private Key
AS	Auction Server
IBE	Identity Based Encryption
MAC	Message Authentication Code
BGV	Brakerski-Gentry-Vaikun-tanathan
TA	Trust Authority
RS Code	Reed-Solomon Code
TSE	Truth Finder for Spatial Events
PTSE	Personalized Truth Finder for Spatial Events
EM Algorithm	Expectation Maximization Algorithm
MAP Estimation	Maximum A Posteriori Estimation
GBC	Generalized Batch Cryptosystem
RPM	Reputation and Pseudonym Manager
TPM	Trust Platform Module
TLS	Transport Layer Security

preference, worker expertise, the availability of sensors, and worker reputation (including honesty and loyalty). WT can help support DT to a certain degree as well.

However, worker selection and task assignment face several security and privacy threats. First, task division and assignment may leak some sensitive task information to malicious workers. Second, workers are required to upload some personal information in the worker selection process. The uploaded information may impact the personal information privacy of workers. Therefore, the information should not be leaked to attackers and SP if the SPs cannot be fully trusted. Third, tasking suffers several kinds of attacks, like Sybil attack and collusion attack. Apart from security and privacy issues, how to guarantee the trust in the selection process is also a crucial issue. MCS workers may intentionally upload fake or cloaked information requested by SP, so that their real personal information will not be revealed. In addition, the SP or end users may also break their commitment or perform worker selection in an unfair way to pursue their own benefits. Therefore, the trust of tasking should be ensured in MCS.

A basic method of worker selection is to calculate a score for each worker according to its preference, interests, ability, location, trust, etc., and decide a worker candidate based on the score [38]–[41]. Based on this idea, when calculating the scores of workers, An *et al.* [38] comprehensively considered a number of properties that affect DT, such as link reliability, service quality, and region heat. However, this scheme does not cover all the impacting factors of DT and WT, e.g., computing abilities and historical behaviors. Therefore, this scheme only supports medium-level of WT and DT. It does not consider false data uploading, and none of other requirements is fulfilled.

Amintoosi and Kanhere [39], [40] proposed a ranking-based scheme that introduces trust and worker ability into the calculation of worker scores. The scheme adopts worker ability of privacy preservation as a factor that influences worker ranking in order to enhance privacy, which helps improve WT. Since the workers with higher trust are more possible to upload data with higher reliability, DT is also improved. This scheme considers both ability factors and trustworthiness of workers. In addition, it also offers a mechanism to resist collusion between workers. When deciding whether a worker should be added into a selected group, SP checks the likelihood of the formation of a colluding group among the selected workers. If the likelihood is beyond a threshold, the candidate worker cannot be added into the selected group. As a result, the scheme supports medium-level WT, medium-level DT, and PT. As these schemes do not consider false data uploading, they provide DT with medium level. However, the privacy issue is not considered in the work. Based on a similar idea, Amintoosi *et al.* [42] further proposed a trustworthy and privacy preserving task assignment in social crowdsourcing. The biggest difference between this scheme and the above one is that when selecting workers, the SP calculates the pairwise privacy score of possible workers, which reveals the ability of privacy preservation. In this way, WT is enhanced with DP provision. However, evaluating a worker's ability for privacy preservation is not an easy task. Besides, the pairwise score evaluated using interaction between two system parties cannot totally reveal the privacy preservation ability. Therefore, only medium-level WT, medium-level DT, and PT are provided. Moreover, none of the above schemes pay attention to the personal information privacy, and the collusion-resist method may also falsely detect collusion attacks. Some socially related workers may probably generate similar data due to the similar habits they have, which should not be thought as collusion. Therefore, this scheme hinders the recruitment of workers by leveraging social networking.

Many papers studied incentive-based tasking schemes to attract workers for massive data collection [37]. Incentive-based schemes usually reward workers with money, services of other types, etc. [43]. In [44], it was proposed to use bitcoins as rewards. Based on game theory, an incentive method measures the abilities of workers, the benefit the MCS SP could get, and the budget of the SP. Based on the measurement, SP then outputs a group of workers. Most of incentive-based schemes utilize an auction model to decide the worker group. In these designs, the uploaded personal information of workers is usually called bidding information.

Nowadays, incentive-based schemes have been widely studied. Some schemes achieve that even with false bidding information, workers cannot increase their rewards [45]–[49]. This helps in resisting the false personal information uploading and providing PT. Zhang *et al.* [50], [51] extended this method and proposed an incentive scheme aiming at discouraging free-riding and false reporting based on game theory. The scheme guarantees that both end users and workers cannot achieve more benefits by breaking their promises and PT is supported as a result. However, the scheme fails to resist DDoS attack, and none of them takes into account the privacy issues. In addition, it is only effective for selfish workers. For malicious attackers with other purposes apart from benefits, it may not work well. Therefore, these schemes can only support WT and DT with a low level.

To protect the personal information privacy, some schemes try to support differential privacy by adding a random perturbation to the bidding information [45], [49], [52]. Based on this idea, Jin *et al.* [49] proposed an incentive-based worker selection and task assignment scheme. This incentive-based tasking scheme mainly explores the differential privacy of bidding information by adding randomization to its outcome. In this way, a change in the bid of one worker would not lead to much change in payment. As a result, it is difficult for a curious worker to infer bidding information of other workers from outcome. Therefore, this scheme can well protect personal information of workers and provide PP. It guarantees that no worker could achieve more benefit by claiming a false bid as well. This prevents false bid submission, which enhances PT to a certain degree. Similar schemes were proposed in [45] and [52].

All the aforementioned methods do not consider verifiability of the selection result. To tackle this problem, some schemes take into consideration SV, and utilize homomorphic cryptography to preserve personal information privacy. In [53], a secure and dependable incentive mechanism was designed based on an optimal omniscient auction model. In this scheme, the crowd of workers is randomly divided into two groups of different sizes. With a constrained budget, the scheme estimates proper unit payment using a small group by maximizing the total revenue that a winner set can obtain, and then uses the estimated unit payment and the left budget to decide the payment for each worker. To prevent SP from forging the payment and to protect the bidding privacy, the SP is required to publish encrypted bids from bidders and encrypted aggregated results to all. After that, the workers in the small groups can verify whether the SP tampers the bid input and whether the result is true or not. This scheme satisfies C/I with the help of homomorphic encryption. Since the payment can be verified, SV is also offered. However, to support SV, it requires all the members of the small group to present their bids honestly, which may not be realistic. To address this problem, the scheme encourages workers to participate in the verification process by offering more payment. However, SP cannot be fully trusted, and internal attacks could occur due to collusion among SP and malicious workers. For example, distrusted SP can request malicious workers in a small group to deny participating in the verification procedure. In this case, verification will fail. As a result, low-level ST is offered.

Sun and Ma [54] proposed a signature and homomorphic encryption-based privacy-preserving verifiable incentive mechanism. Auction issuer (AI) maintains a bulletin board, and all public information can be published on it. The scheme introduces a trustworthy party AI in an MCS system. When a worker uploads its bid, it also makes a commitment on its bid. The commitment can be used to verify whether the worker has uploaded this bid. To protect privacy, the commitment needs to be encrypted by workers, and the commitment will not be open until the task is finished. However, the worker may collude with SP and reject to open the commitment after the task. To tackle this problem, the authors introduced time-lapse cryptography (TLC) service. TLC is offered by AI, and the workers encrypt the commitment with time-lapse public key issued by AI. When worker selection is finished, AI issues corresponding time-lapse private key to decrypt the commitment. In this way, the scheme can support Nr and is able to resist collusion attack. After receiving bidding information and associated commitment, SP decides the payment for the worker and returns a receipt to the worker. The worker can verify whether the payment is calculated by following a predefined protocol by decrypting all the encrypted commitments. Even SP colludes with workers or end users, it cannot forge the amount of payment. Therefore, RV and high-level ST are supported. The encryption of bidding information helps realize C/I.

Dimitriou and Krontiris [56] proposed a pseudonym-based security framework for implementing an incentive mechanism. The main idea of the scheme is to attach a unique signature of the worker to its encrypted bids. In the scheme, the workers first send a commitment on its bid to an auction server (AS). However, AS cannot extract the bid until an opening process. Once the AS is able to read the bids, it can choose a winner set and publish it in a bulletin board with a signature. Similar to the scheme in [53], the scheme considers C/I, Au, medium-level WT, medium-level DT, PP, IP, Nr, SV, and RV.

Apart from applying homomorphic encryption to protect personal information, there are some other popular methods that were applied to protect personal information privacy of workers, e.g., uploading cloaked information, adding random noise, and clustering workers into one group to support *k*-anonymity or differential privacy [43], [57]–[62]. These methods reduce the precision of uploaded information. Without carefully processing, these methods could have a side impact on worker selection. Many schemes apply the above methods into the protection of location privacy in MCS, which is required in many applications, such as transportation monitoring. In the incentive-based tasking scheme designed by Wu *et al.* [43], workers join a clustering group to support *k*-anonymity. In this way, PP and IP is protected. Pournajaf *et al.* [59], [60] proposed a task assignment method for spatial sensing task assignment with cloaked location information. The scheme introduces a task server that estimates location distribution with the cloaked information for task assignment. To improve assignment accuracy, workers need to perform local processing and to decide where to sense data. This method could protect worker location privacy to a certain degree. However, if the workers cloak their location information too much, the method may fail, thus PP is not well enhanced. In [61], a scheme to support location privacy preservation was proposed. It divides a whole sensing area into several subareas based on privacy budget and random noise. Then, each subarea is divided into several areas randomly.

For each area, there exists at least one worker with a high probability. The worker could transmit the sensed data to the requester with the help of a centralized server or through MANET. Similarly, in [63], a scheme that supports differential location privacy was proposed, which applies a contour plot to demonstrate the density distribution of workers, and adds a random noise to their location information. In [62], workers are allowed to upload generalized location information rather than the accurate location in order to protect personal location information and support k-anonymity. Most of these schemes fulfill PP, IP, and C/I. However, none of the schemes consider other personal information except for location privacy. Additionally, SV and RV of selection are not considered.

Krontiris and Dimitriou [35] proposed a worker selection scheme that considers both privacy of workers and that of end users. The scheme enables end users to select workers based on their own criteria, and only the mobile users fulfilling their criteria can access their data. The scheme protects the location privacy and the identities of workers by introducing cloud agents, which act as the interference of workers thus hiding the concrete locations and identities of workers. Since the end users can choose workers based on their attributes, this scheme provides AC and TP. Similar schemes were proposed in [35]. In [64], personal information privacy is protected by sharing generalized information rather than precise one with SP. The workers are allowed to choose a privacy level by themselves. As a result, PP is provided. A similar scheme was proposed in [65].

Apart from the above schemes, there are some other schemes designed for privacy-preserving tasking. Wang *et al.* [55] proposed an incentive-based scheme and introduced reputation to it to guarantee WT with medium level. Ye *et al.* [66] designed a context-trust-based worker selection method. This scheme comprehensively considers the influence of task types, difficulty, and payment amount to a worker. By combining all the influencing factors and the historical behavior of a worker together, the scheme can determine the context trust of the worker and figure out whether its claim is trustworthy. In this way, the scheme can choose workers based on task information and WT. It supports medium-level WT, and PT, which further ensures DT to a certain degree. Ni *et al.* [122] proposed an anonymous and location-based worker selection scheme. The authors adopted a matrix to check whether a worker is located in a targeted sensing area without knowing the exact locations of workers. The data is uploaded in an encrypted form. As a result, the scheme fulfills C/I, PP, and IP, but not any other requirements. Huang *et al.* [125] proposed to prevent tracking and ensure identity privacy by frequently changing pseudonym. In this scheme, PP and IP are fulfilled to a certain degree. Duan *et al.* [126] designed a distributed worker selection framework that maximizes social welfare. In their scheme, the result of worker selection is computed locally by workers rather than globally by centralized parties. It hence achieves privacy preservation since mobile users do not need to expose their personal information during task allocation. The scheme achieves PP to a certain degree. Another distributed worker selection scheme was proposed in [127]. The authors introduced several semitrusted nodes in place of a fully trusted authority. Worker are divided into several groups linked with semitrusted parties. The bid of each worker is disguised and shared within group. In this way, PP is achieved to a certain degree.

B. Secure Data Aggregation

Data aggregation is an important data processing step for getting data statistics. It can protect original data privacy to some extent by combining all data. Because the process of data uploading suffers several attacks and SP cannot be fully trusted by workers, it is necessary to guarantee the DP of workers against attackers and SP. Two of the most popular techniques for privacy-preserving data aggregation are homomorphic encryption [67], [69], [71], [75] and adding random noise/perturbation to data [68], [71]–[74]. Both allow the SP to aggregate the data without knowing the content of them. Some schemes introduce additional technologies about pseudonym and trust to enhance security, privacy, and trust in the process of data aggregation [69].

In [67], a data aggregation scheme was proposed based on additively homomorphic identity-based encryption (IBE). The data reported to SP should be encrypted with the private keys of workers. Then, the SP can aggregate the data without knowing their contents. This scheme also introduces a trusted third-party, named registration authority to handle the registration of participating parties and to issue IBE keys to the workers. The underlying encryption algorithm guarantees that even some of the workers collude with SP or end users, they cannot decrypt the encrypted data, thus resist collusion attacks. This scheme guarantees C/I, Au, but cares little about trust issues.

Chen *et al.* [68] proposed a data aggregation scheme to support privacy preservation and data integrity. Diffie–Helman cryptography was adopted to guarantee confidentiality. Integrity was supported by attaching a homomorphic message authentication code to each message. By adding a random noisy value to each data message, data privacy is supported. In this scheme, the distribution of noise is carefully selected to guarantee differential privacy, and thus it can support high-level data privacy. Moreover, all workers are divided into several groups and the workers of the same group are organized to form a ring, which is managed by a group manager.

Another scheme based on Brakerski–Gentry–Vaikuntanathan homomorphic encryption was proposed in [69]. This scheme introduces a trust authority to perform identity and key management. In the scheme, ring signature is adopted to protect the identities of workers for achieving anonymity. The scheme also offers a verification mechanism. It enables end users to verify the correctness of aggregation results of the collected data by utilizing homomorphic encryption and homomorphic hash function. Since data is transmitted in a form of cipher text, DP can be ensured. The scheme also supports other functions apart from sum, such as mean and variance.

Xie *et al.* [70] considered both data privacy and location privacy in data aggregation. The authors anonymized location information to support location privacy, and utilized erasure codes, such as Reed–Solomon code, to slice data reports to support *k*-anonymity. As a result, this paper supports IP, DP, and partial location information privacy. In [71], both homomorphic encryption and data cloaking were adopted to support differential privacy of data report and C/I.

In [72], a personalized privacy-preserving data aggregation scheme was proposed for histogram estimation. Workers can choose privacy levels according to their own strategies. In this scheme, an aggregator is not trustworthy. To guarantee data privacy, the workers first decide some parameters based on their own privacy strategies for a bloom filter, which is used to generate a random response to the request of the aggregator. In this way, the scheme supports local differential privacy, and the data is confidential even for the aggregator.

Some schemes support DP by adding random perturbation to sensory data [73], [74]. In this way, attackers cannot obtain the real truth of data reports unless they get a large number of data reports. Even with a number of data reports, the attackers can only obtain the content of the aggregated result and cannot get the concrete content of a single report uploaded by a worker. In this way, DP is guaranteed to a certain degree.

A cloud-enabled privacy-preserving data aggregation method was proposed in [75]. This scheme adopts worker reliability as an impact factor, and uses homomorphic encryption to protect both sensed data privacy and privacy of reliable information. However, this scheme requests interaction between a cloud and users to generate a final aggregated result, which may introduce extra communication overhead.

C. Truth Discovery

Truth discovery in MCS is mainly about dealing with the false reports and discovering truth from noisy reports with various reliability and trust. A fine truth discovery should first of all guarantees DT and WT, which is its primary goal. That is, even some of collected reports are unreliable, the final result generated by SP should still be of high reliability, and the truth can be found. In this process, privacy issues and security issues should also be paid attention to.

A common method of truth discovery is voting. In practice, there may be several observers in terms of a same target. Voting-based truth discovery schemes take observed results with the most observers as the truth. In [80], a voting-based truth discovery method was proposed. The adoption of voting offers DT in a medium level. The scheme further adopts random perturbation to support differential data privacy, and thus provides DP. However, this voting-based method requires that the number of observers to be big enough, which could be costly and increase extra communication overhead. Similarly, Ren *et al.* [107] proposed to evaluate the reputation of an MCS report based on the amount of supports and conflicts it obtains from other sensing reports.

Another idea is to compare required context information (location information, for example) to generate a report with inferred context to determine the trustworthiness of a report. Based on this idea, Quyang *et al.* [76] studied the process of how a crowdsourced report is generated. In order to make a report, a worker must physically present at a certain location to observe whether there is any target event. With this analysis, the authors proposed two new unsupervised models [i.e., truth finder for spatial events (TSE) and personalized TSEs]. SPs utilize the two models to evaluate location popularity, a worker's location visiting indicators, event labels, worker reliability, and crowdsourced reports. With the evaluated results, SPs are able to decide the trustworthiness of the worker that validates whether a report is generated by a certain worker as desired. This method can detect false data only in the case that an attacker uploads data at a false location. Even we ascertain that a worker is present at a certain location where its report is generated, we could not determine whether this report is tampered or not. Therefore, this scheme can only guarantee low-level DT, and cannot satisfy any other requirements on DT. Besides, privacy issues are not considered much in this scheme.

Several context-aware schemes were proposed in the literature. Kurve *et al.* [77] proposed an MCS context-aware incentive method, which introduces a cloud platform. Two mobility-aware schemes were proposed in [78] and [79], which take into account the context or mobility trajectory of workers to decide the likelihood that a worker has actually generated the sensing report it uploads. Just like the work in [76], only low-level DT is offered, and these schemes lack the consideration of security and privacy issues.

Wang *et al.* [86] proposed to utilize a maximum likelihood estimation approach in truth discovery. The authors considered two main variables that influence generated reports, namely sensor reliability and real truth. The scheme adopts an expectation maximization (EM) algorithm to estimate the real truth based on maximum likelihood estimation. Although the scheme comprehensively considers the two factors that affect sensed data reports, the trust of workers is not taken into account, which is hard to predict. Therefore, the scheme supports medium-level DT. Kubota and Aritsugi [15] further improved the above scheme and proposed a new one to support an online data arrival model. The EM algorithm was also adopted, which improves effectiveness by inserting ground truth. A similar scheme was proposed in [82], which uses maximum *a posteriori* estimation to find the truth in a quantitative claim system and utilizes bias and confidence to evaluate the ability of workers. Wang *et al.* [114] also proposed a truth discovery mechanism to handle the situation that the data reports arrive continuously. They pointed out that in some cases, the reliability of individual sources is usually some unknown priori. To tackle this problem, they introduced reputation scores of workers and adopted the EM algorithm to estimate the real truth in a recursive way. Therefore, the scheme supports DT with a medium level. The likelihood analysis-based truth discovery methods support DT. However, few of the existing schemes consider privacy issues.

Zhang *et al.* [83] proposed a ground truth (i.e., real truth) inference scheme for a multiclass labeling system based on machine learning. Its main idea is to utilize the multiple noisy label sets of examples to generate features. Then, it uses a K-means algorithm to cluster all examples into k different groups, each of which is mapped to a specific class. But the scheme does not consider the influence of WT, thus could only support medium-level DT. However, none of other requirements are fulfilled by this scheme.

Prandi *et al.* [84] proposed a path discovery application based on both MCS and traditional online crowdsourcing. The scheme evaluates data trustworthiness by comparing the collected data with a gold data set in which the data is authorized and correct. In the absence of the gold data set, the data is evaluated by a voting system based on the feedback from end users. By considering the reputation of end users, the scheme guarantees DT to a certain degree. The truth discovery based on a gold data set could support DT with a high level. The concept of gold data set is also adopted by Drosatos *et al.* [85]. The authors designed a voting-based scheme. In addition, fully trustworthy workers called anchors are set to help improving the trustworthiness of the whole system.

In [87], a trust assessing framework was proposed for inferencing with uncertain streaming information. It treats streaming data from different organizations with different trust levels for verifying the correctness or quality of an inference. The scheme is designed for the verification on an inference and the adoption of WT. DT measurement helps enhance DT validation. However, the scheme ignores the privacy issues in MCS truth discovery.

Meng *et al.* [88] proposed an effective optimization-based framework to solve the problem of truth discovery for crowd sensing of correlated entities. The scheme considers real truth and sensor reliability as two variants. Different from the work in [81], the authors considered the influence of data correlation and tackled the problem by clustering the sensors into disjoint independent groups based on their relationships. Hamm *et al.* [90] proposed to utilize perturbation to support differential privacy of sensed data.

Meng *et al.* [89] explored observation sparsity and redundancy issues in MCS. The authors pointed out that there are usually several participants observing a same entity, and sometimes, the observation of an entity by a participant may be missing. The authors proposed to first estimate the missing observation values and then aggregate observations of the same entity together. With this way, the truth of an entity is estimated with high reliability.

To better deal with the big data collected by workers, Zhuo *et al.* [121] introduced a cloud-based solution to reduce computation burden. The collected data are encrypted, and only valid end users can request the data. Thus, this solution achieves C/I, DP, and AC. The cloud also generates proofs during computing. With these proofs, end users are able to verify the correctness of final computation results. Therefore, PV is fulfilled. The scheme does not fullfil other requirements.

Zhou *et al.* [124] proposed a framework called FIDC for improving data credibility. The scheme adopts a clustering algorithm to analyze correlation characteristics of collected data. In this way, it can defend against collusion attack and potential data falsification threats attack, and thus achieves DT with high level.

D. Access Control

In an MCS system, the workers need to request for some task information. However, for the sake of privacy protection, end users may not be willing to provide their task information publicly. In this case, it is expected that only the valid workers are allowed to access this information. Apart from the data privacy of end users, the sensed data provided by workers should also be protected from leaking to malicious parties. AC aims to prevent illegal access to the task information. Thus, applying AC can support TP and DP. Currently, there are many AC schemes proposed.

Ye *et al.* [91] proposed a context-aware fine-grained AC scheme for the data stored in mobile devices. The authors considered that sensed data, like audio may contain sensitive information concerning worker privacy. Moreover, the contextual information included in the sensed data may reveal sensitive information of other parties apart from workers. For example, if a worker uploads a photograph of his environment, the private information of the corporation where he works may be leaked. To tackle this problem, Ye *et al.* [91] set a binary context attribute group for the collected data, and leveraged machine learning methods to decide the attribute group of the data. The attribute group enables a manager to decide whether the data is allowed to be uploaded to a server [91]. The scheme supports AC and DP.

Some schemes introduce trust or reputation into AC. Folorunso and Mustapha [92] considered both WT and expertise level of a worker to perform data AC. Only the trustworthy workers with enough expertise can access the data. In this way, the scheme guarantees DP, AC, and WT to a certain degree. Chang *et al.* [93] proposed a flexible and adaptive AC scheme for crowdsourcing systems named TrustForge. The scheme combines policy-based AC and reputation-based AC by setting reputation as an attribute of worker. The reputation of worker is calculated according to data quality. The scheme supports low-level DT and AC.

Choi *et al.* [94] tried to solve the issue of data AC in a decentralized manner. They argued that there exists single point failure risk if all sensed data is stored in a centralized server. Therefore, they proposed to adopt several distributed remote storages. In this scheme, a broker is introduced to manage the data. A worker can decide its AC policy by itself. This scheme AC scheme can prevent illegal access to both sensed data and workers' personal information such as identity and location. Therefore, this scheme supports DP and AC.

Zhou *et al.* [95] proposed an efficient generalized batch cryptosystem (GBC) to support both batch encryption and decryption for any public key encryption algorithms. GBC enables that only the data requesters with certain attributes can decrypt encrypted data. With GBC, an attribute-based AC scheme for secure file sharing in a cloud-assisted MCS system can be developed. The scheme supports C/I, AC, and DP.

Dimitriou *et al.* [96] explored task information privacy by applying a decentralized MCS architecture. In the scheme, with the help of tokens issued by SP, the end users obtain data from workers directly. In this way, only the end users fulfilling certain requirements can access the data. The end users can select workers based on their own policies. Therefore, the task information is only the selected group of workers. We can see that the task information is protected to a certain degree and the scheme supports TP and AC.

Boutsis and Kalogeraki [97] proposed to store data locally in users' personal devices and keep personal information among multiple user databases. As a result, in the sight of attackers, the data stored by users has equal probability to contain sensitive information, thus this method provides DP and AC in terms of storage.

E. Trust Management

Trust plays an important role in MCS systems. Trust management helps SP offer sound services by selecting trustworthy workers to generate reliable data. In MCS, both DT and WT should be evaluated. When evaluating a worker's trust, the MCS systems should take into account many properties related to the worker, e.g., historical behaviors, sensed DT, and worker abilities (such as computing ability, sensor availability, communication capacity, and user expertise). Trust evaluation and management can provide WT and facilitate DT. Since trust evaluation and management request collecting the behavior and personal information of workers, PP and IP should be paid attention in this process.

Amintoosi and Kanhere [98], [99] proposed a reputation framework for social crowdsourcing systems based on fuzzy logic for the evaluation of DT. The framework comprehensively considers quality of contribution and trust of a worker. Besides, it also takes into account the impact of such properties as data quality, worker locality, link reliability, expertise, time decaying, friend gap, and so on. The scheme guarantees DT with a medium level. The trust of data could be further utilized to evaluate the reputation of workers together with the feedback from end users. Therefore, the scheme also supports high-level WT.

Wu *et al.* [100] proposed a novel endorsement-based reputation system to evaluate the trust of workers, which takes endorsement of other workers into account. In the scheme, an endorsement Web is first of all built to reveal the endorsement relationship between workers. Then, to assess the reputation of a worker, the evaluator would turn to all the workers it endorsed to predict the target worker's expertise by leveraging collaborative filtering. Furthermore, the feedback of performance from users is used to adjust trust evaluation results. With the expertise taken into consideration, the reputation of the target worker is assessed. Since the scheme considers both worker expertise and user feedback, it supports WT and DT with a medium level.

Manzoor *et al.* [101] computed the trust value of a worker using predications and user feedback. The trust manager performs error analysis, and leverages analysis results to evaluate the quality of contributions. The trust value of a worker is decided by the current and historical data quality as well as the results of DT evaluation in the past. This scheme considers the DT, however, the trust of the worker is ignored. The DT alone may not represent the trust of a worker. Therefore, it cannot accurately evaluate WT.

Vaya [102] proposed a robust reputation mechanism for MCS. The scheme mixes gold tasks with normal tasks, and issues them to workers together. The gold task is a kind of tasks for which the correct result has been computed or known by SP ahead of time. The results of these gold tasks provided by workers would be compared with the precomputed results to reveal the current contribution quality of workers. The trust score of a worker is decided by current DT and historical DT, which is computed with the number of successfully completed tasks and the total number of assigned tasks. This scheme can support high-level DT. The trust of worker is calculated by considering the historical and current performance of the worker, and it supports medium-level WT.

Ceolin *et al.* [103] considered data provenance, which is considered as the source information about entities, activities, and people involved in producing a piece of data or thing. Data provenance can be used to form assessments on data quality, reliability or trustworthiness. Ceolin *et al.* [103] proposed a reputation and provenance-based trust assessment scheme for the collected data. This scheme comprehensively considers worker reputation, its abilities, and sensing conditions, thus it supports DT in a medium level. A similar scheme was proposed in [104].

To protect the privacy of workers in trust evaluation, Christin *et al.* [105] proposed a pseudonym-based scheme that leverages cloak to prevent the leakage of collected data, in which a tradeoff is made between the accuracy of evaluation and the privacy. The scheme could resist such attacks as Sybil attack, replay attack, etc. Huang *et al.* [106] showed that two challenges in MCS are data trustworthiness and worker privacy. They proposed one solution that utilizes reputation as criteria to evaluate contribution reputation. The above two schemes offer A/D, IP, PP, and WP with a medium level. However, the method proposed in [105] suffers from several drawbacks. The reputation is in conflict with pseudo-identities, and using historical behaviors to evaluate the reputation of a worker would harm its privacy. To address these problems, a pseudonym-based identity preserving scheme was proposed, in which a trusted third-party is introduced to map the reputation to workers' new pseudonym [34].

F. Secure and Privacy-Preserving Data Reporting

Data reporting is the process of uploading the data from workers to SP, which includes data encryption, provenance authentication, secure routing, key exchange, etc. Data conveyed via MCS can be protected with encryption, data cloak, data generalization, etc. In this process, data confidentiality, integrity and provenance authentication should be guaranteed. In a centralized MCS architecture, data is usually considered to be transmitted to SP directly, and current work tends to utilize data encryption to guarantee C/I.

In [108], data generalization is applied to support k-anonymity, which supports DP. In this scheme, workers change their pseudonym periodically. The worker generates a new key pair for this pseudonym, and a trusted authority called reputation and pseudonym manager (RPM) is introduced to sign the public key by applying a blind RSA signature mechanism to provide Au for the pseudonym and key pair. The signing key of RPM also changes periodically. As a result, the worker uses the blindly signed pseudonym and the newly generated private key to report sensor readings and to transfer reputation to its next pseudonym. To prevent attacks by maliciously tracking workers or by linking pseudonyms of different periods through reputation values, the reputation value of each worker is generalized and cloaked. In this way, the anonymity and identification of workers are guaranteed. The introduction of RPM further supports Au and Nr.

Dua *et al.* [109] turned to trust platform module (TPM) to solve the problem of integrity guarantee. With TPM, the scheme guarantees that the data cannot be tampered by malicious workers. Gisdakis *et al.* [110] introduced a trusted third party for the purpose of identity and key management. The adoption of pseudonym well protects the identity privacy of workers. C/I and Au are supported by authenticated transport layer security channels established between different MCS entities.

Qiu *et al.* [111] proposed SLICER, which is one of the first *k*-anonymous privacy-preserving schemes for crowdsourcing of multimedia data. SLICER integrates a data coding technique and message transfer strategies to support strong protection of participants' privacy, while maintaining high data quality [111].

Pournaras *et al.* [112] proposed a ubiquitous social mining method via modular and compositional virtual sensors, which takes MCS as a data source for a planetary nervous system. The data is collected via a decentralized method. The main idea for privacy preservation is when designing virtual sensors, a filter is involved for the purpose of AC, which means that the data is only available for the virtual sensors that fulfill specified requirements. However, the virtual may not be trustworthy or secure enough, therefore, although the data privacy is considered, it is not well protected.

V. Open Issues and Future Research Directions

A. Open Issues

According to the above analysis and comparison as summarized in Table V, we figure out a number of open issues in MCS.

First, truth discovery still needs to be further explored. As aforementioned, a lot of tampered, unreliable, cloaked data exist. Specially, with personal privacy concerns, it is possible that workers upload cloaked or tampered data to SP. Current truth discovery methods measure the trust of data reports in an indirect way by considering various influencing factors, such as worker trustworthiness, ability and reliability. Based on this idea, many algorithms were developed [15], [81], [86], [108], e.g., voting-based methods [80], [84]. However, they often ignore the privacy issues. From Table V, we can see that few truth discovery schemes guarantee DP and PP. Besides, the literature still lacks truth discovery methods that analyze the intrinsic properties of data in different application scenarios and need the methods that measure DT and find real truth based on data analysis results. In addition, most of the current methods cannot well deal with distrusted and tampered data. How to find the truth from unreliable data reports by exploring the intrinsic properties between data is still an open issue.

Second, verifiability on the output result provided by SP is not supported by most of the current schemes. For an end user who turns to the SP to complete a certain task, it is reasonable to provide him with a mechanism to verify the correctness or quality of the final result. Verifiability of the final result will enhance user trust in the SP. However, few schemes support verifiability on final results. In practice, verifiable computation or evaluation or auditing on the final result outputted by the SP should be well supported.

Third, most of the literature concentrates on the centralized architecture of MCS, where SP is a centralized server. Only a few studies consider a decentralized architecture of MCS, in which SP is acted by several distributed agents. Moreover, few work pay attention to a fully distributed MCS architecture. There exist serious security, privacy, and trust issues in fully distributed MCS. In the centralized architecture, the data is considered to be transferred to the SP through secure channels, and it is easy to realize key management. However, it is more complex to perform identity and key management, trust management, secure data uploading, secure routing, data aggregation, and data fusion in a distributed environment. How to build a secure, privacy-preserving, and trustworthy MCS system in a distributed way is another open and interesting issue.

Fourth, data processing by workers is not fully explored. Collected data may contain sensitive information of workers. If this information is not protected, the risk of privacy disclosure will be increased. On the other hand, the uploaded data may contain extra information that is not needed by the task. How to exclude sensitive or unnecessary data should be studied. Furthermore, data collected through MCS may contain duplicated data. Many workers may upload the same or similar data to the SP. The duplicated data not only influences the efficiency of data processing like truth discovery, but also increases communication overhead. Therefore, attention should also be paid to data duplication. Data aggregation and data fusion with deduplication should be further explored.

Finally, there are only few researches paying attention to secure data reporting. Authentication on data reporting, especially authentication on data provenance and DT, is seldom considered. Specially, their relative identity and key management issues are seldom investigated. Provenance authentication can provide Nr and help improve revocation (Re), and thus becomes a significant mechanism to build up a trustworthy MCS system.

B. Future Research Directions

Before concluding this survey, we propose a number of interesting future research directions in the field of MCS security, privacy, and trust in order to motivate innovation and special efforts. These directions also stimulate our future research work.

1) Truth Discovery With Privacy Preservation: Truth discovery is expected to be performed in a privacy-preserving

TABLE V
COMPARISON OF EXISTING WORK BASED ON PROPOSED REQUIREMENTS

Reference	Category	C/I	Au	WT	DT	PT	ST	Pr				A/D	Nr	Re	V			AC
								PP	DP	TP	IP				SV	PV	RV	
[38]	Tasking	N	N	L	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[39][40]		N	N	H	M	Y	N	N	N	N	N	N	N	N	N	N	N	N
[42]		N	N	H	M	Y	N	N	N	N	N	N	N	N	N	N	N	N
[43]		N	N	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N
[60]		N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
[61]		N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
[62]		Y	N	N	N	N	N	Y	N	N	y	N	N	N	N	N	N	N
[35, 36]		N	N	N	N	N	N	Y	N	Y	N	N	N	N	N	N	N	N
[122]		Y	N	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N
[125]		N	N	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N
[127]		N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
[46-48]	Incentive	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
[50, 51]		N	N	L	L	Y	N	N	N	N	N	N	N	N	N	N	N	N
[45, 49, 52]		N	N	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N
[53]		Y	Y	M	L	N	H	N	N	N	Y	Y	N	N	Y	N	Y	N
[54]		Y	Y	M	M	N	M	Y	N	N	Y	N	Y	N	Y	N	Y	N
[56]		Y	Y	M	M	N	M	Y	N	N	Y	N	Y	N	Y	N	Y	N
[64, 65]		N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	N
[55]		Y	Y	M	M	Y	M	Y	N	N	Y	N	N	N	Y	N	Y	N
[126]		N	L	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
[93]	Access Control	N	N	M	L	N	N	N	N	N	N	N	N	N	N	N	N	Y
[91]		N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y
[92]		N	N	M	L	N	N	N	N	N	N	N	N	N	N	N	N	Y
[94]		N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y
[95]		Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y
[96]		N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y
[97]		N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y
[67]	Data Aggregation	Y	Y	N	N	N	N	N	Y	N	Y	Y	Y	N	N	N	N	N
[68]		Y	N	N	N	N	N	N	Y	N	N	Y	N	N	N	Y	N	N
[69]		Y	N	N	N	N	N	N	Y	N	Y	Y	Y	N	N	Y	N	N
[70]		N	N	N	N	N	N	Y	Y	N	Y	N	N	N	N	N	N	N
[71]		Y	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	N
[72]		Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
[73]		N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
[74]		N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
[75]		Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
[98, 99]	Trust Management	N	N	H	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[100]		N	N	M	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[101]		N	N	L	L	N	N	N	N	N	N	N	N	N	N	N	N	N
[102]		N	N	M	H	N	N	N	N	N	N	N	N	N	N	N	N	N
[103, 104]		N	N	M	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[105, 106]		N	N	M	L	N	N	Y	N	Y	Y	N	N	N	N	N	N	N
[48]		N	N	L	N	N	N	N	N	N	N	N	N	N	N	N	N	N

(Continued)

way. This is because, for one thing, most of data collected in MCS is related to the privacy of workers. For another thing, SP is generally supposed to be not fully trusted and curious about the privacy of workers. Till now, although many truth discovery schemes have been proposed based on various methods, most of them do not consider the privacy issues. Therefore, it is significant to study how to find the truth meanwhile protecting worker privacy.

2) Truth Discovery in Various Application Scenarios: Current truth discovery methods usually measure the trust of contributions of workers by evaluating their ability, reliability, etc. However, data reports provided by workers may have specific intrinsic properties in different application scenarios, with which more reliable and trustworthy truth discovery can be offered. However, few studies pay attention to a truth discovery method by exploring the intrinsic properties between

TABLE V (Continued)
COMPARISON OF EXISTING WORK BASED ON PROPOSED REQUIREMENTS

[80]	Truth Discovery	N	N	N	M	N	N	N	Y	N	N	N	N	N	N	N	N	N
[84]		N	N	Y	H	N	N	N	N	N	N	N	N	N	N	N	N	N
[76-79]		N	N	N	L	N	N	N	N	N	N	N	N	N	N	N	N	N
[86]		N	N	Y	H	N	N	N	N	N	N	N	N	N	N	N	N	N
[83]		N	N	N	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[15, 81, 82]		N	N	N	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[80]		N	N	N	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[107]		N	N	L	M	N	N	N	N	N	N	N	N	N	N	N	N	N
[121]		Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	Y
[124]		N	N	L	H	N	N	N	N	N	N	N	N	N	N	N	N	N
[108]	Data Reporting	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
[110]		N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N

Tasking contains both worker selection and task assignment;
Incentive refers to incentive based worker selection and task assignment;
Y means the scheme achieves the corresponding requirement;
N means the scheme does not achieve the corresponding requirement;
H/M/L respectively means the scheme achieves the corresponding requirement at a high/medium/low level.

data reports, and no related truth discovery model was proposed, which is a significant topic. How to create a generic and pervasively feasible model for truth discovery that can be applied in various application scenarios is worth our investigation.

3) Verifiable Data Processing by MCS: As aforementioned, few existing schemes have paid attention to the verifiability and quality of the outcome presented by SP, as well as the fairness of worker selection and correctness of reward payment. How to offer verification and perform auditing in MCS is seldom explored in the past literature. However, verification and auditing on computing results, tasking fairness and reward execution can greatly help end users make a wise choice among several SPs, enhance user trust and WT in MCS and benefit its practical adoption. Obviously, due to the lack of computing ability and actual information, it is very challenging to support auditing, evaluation or verifiability on the result outputted by SP. In our opinion, it is significant to explore the methods to support verifiability in MCS with regard to SV, PV, and RV.

4) Countermeasures in Fully Distributed MCS Architecture: Distributed MCS architecture is a promising platform for MCS services, in which SP is implemented by a single mobile node or several mobile nodes rather than a server. With the popularity of mobile devices and mobile social networking, it is possible that mobile end users turn to distributed SPs for help by utilizing their social associations. In this case, the security, privacy, and trust issues in MCS are becoming more complex, which are different from those in the case that the SP is acted by a server. Therefore, relative countermeasures, like authentication, trust management, data aggregation, data fusion, etc. should be seriously studied in such a distributed architecture. More interesting schemes should be innovated to support distributed and ubiquitous MCS applications and services.

5) Trustworthy and Privacy-Preserving Data Fusion: Data fusion is very helpful to support efficient data analysis and real truth discovery. It integrates various data into a consistent, accurate, and useful representation. However, collected data in MCS normally varies in trust, quality, and reliability, which increases the difficulty of data fusion. Data provided by different MCS workers may contain duplicated information as well. Furthermore, it is also quite usual to process data locally at workers to remove duplicated, useless or sensitive information. Therefore, data fusion becomes challenging in MCS since it should be able to deal with data variety, data duplication, useless data, and sensitive information at both worker side and SP side. How to support trustworthy data fusion in order to ensure the data set quality after fusion and how to preserve sensitive data privacy during data fusion are interesting future research topics.

6) Trustworthy Provenance Authentication With Privacy Preservation: Provenance authentication helps verify the validity and trust of data reports, which helps SPs choose data accordingly. Considering the privacy issues in MCS, it is crucially important to offer data provenance by preserving the privacy of workers simultaneously, especially for identity privacy. Since DT is highly related to WT, the authentication on the WT with privacy preservation is also important. Important as it is, this paper pay little attention to anonymous authentication on different types of trust in MCS. However, it is a promising topic for building up a secure and trustworthy MCS system with privacy preservation.

VI. CONCLUSION

MCS has emerged as an effective and efficient method for data collection and processing due to its ubiquity and flexibility. Despite the great benefits it brings, MCS still faces many problems in terms of security, privacy, and trust, due to its nature of openness and unreliability. There are still some issues that have not yet been deeply investigated in academia and industry. In this paper, we performed a thorough survey on the security, privacy, and trust in MCS. We introduced the basic architectures of MCS and analyzed the specific characteristics of MCS by comparing MCS with WSN and traditional online crowdsourcing. Based on the threat analysis, we further proposed the requirements for establishing a secure, privacy-preserving and trustworthy MCS. Taking the requirements as essential criteria, we extensively reviewed the current literature and commented the pros and cons of existing work. Finally, we explored the open issues that have not yet been seriously investigated and proposed a number of research directions to stimulate future efforts.

REFERENCES

[1] C. Hu, P. Resnik, and B. B. Bederson, "Crowdsourced monolingual translation," *ACM Trans. Comput. Human Interact.*, vol. 21, no. 4, pp. 1–35, Aug. 2014, doi: 10.1145/2627751.

[2] C. Chen *et al.*, "Interactive crowdsourcing to spontaneous reporting of adverse drug reactions," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 4275–4280, doi: 10.1109/ICC.2014.6883992.

[3] S. Hu, L. Su, H. Liu, H. Wang, and T. F. Abdelzaher, "SmartRoad: Smartphone-based crowd sensing for traffic regulator detection and identification," *ACM Trans. Sens. Netw.*, vol. 11, no. 4, pp. 1–27, Dec. 2015, doi: 10.1145/2770876.

[4] V. Pankratius, F. Lind, A. Coster, P. Erickson, and J. Semeter, "Mobile crowd sensing in space weather monitoring: The Mahali project," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 22–28, Aug. 2014, doi: 10.1109/MCOM.2014.6871665.

[5] J. McCrae, N. J. Mitra, and K. Singh, "Surface perception of planar abstractions," *ACM Trans. Appl. Perceptive*, vol. 10, no. 3, pp. 1–20, Aug. 2013, doi: 10.1145/2501853.

[6] J. Sun and H. Ma, "Collection-behavior based multi-parameter posted pricing mechanism for crowd sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 227–232, doi: 10.1109/ICC.2014.6883323.

[7] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 360–368, Aug. 2014, doi: 10.1109/JIOT.2014.2337886.

[8] C.-C. Wu, K.-T. Chen, Y.-C. Chang, and C.-L. Lei, "Crowdsourcing multimedia QoE evaluation: A trusted framework," *IEEE Trans. Multimedia*, vol. 15, no. 5, pp. 1121–1137, Aug. 2013, doi: 10.1109/TMM.2013.2241043.

[9] Y. Baveye, E. Dellandréa, C. Chamaret, and L. Chen, "LIRIS-ACCEDE: A video database for affective content analysis," *IEEE Trans. Affect. Comput.*, vol. 6, no. 1, pp. 43–55, Jan./Mar. 2015, doi: 10.1109/TAFFC.2015.2396531.

[10] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016, doi: 10.1109/ACCESS.2016.2519820.

[11] C. Wang, H. Liu, K.-L. Wright, B. Krishnamachari, and M. Annavaram, "A privacy mechanism for mobile-based urban traffic monitoring," *Pervasive Mobile Comput.*, vol. 20, pp. 1–12, Jul. 2015, doi: 10.1016/j.pmcj.2014.12.007.

[12] L. Tan *et al.*, "Mining myself in the community: Privacy preserved crowd sensing and computing," in *Proc. Int. Conf. Wireless Algorithms Syst. Appl. (WASA)*, Bozeman, MT, USA, 2016, pp. 272–282, doi: 10.1007/978-3-319-42836-9_25.

[13] S. Parthasarathy and T. Hasan, "Automatic broadcast news summarization via rank classifiers and crowdsourced annotation," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, 2015, pp. 5256–5260, doi: 10.1109/ICASSP.2015.7178974.

[14] T. Zhu, J. Behar, T. Papastylianou, and G. D. Clifford, "CrowdLabel: A crowdsourcing platform for electrophysiology," in *Proc. Conf. Comput. Cardiol. (CINC)*, Cambridge, MA, USA, 2014, pp. 789–792.

[15] T. Kubota and M. Aritsugi, "How many ground truths should we insert? Having good quality of labeling tasks in crowdsourcing," in *Proc. IEEE Conf. Comput. Softw. Appl. Conf. (COMPSAC)*, Taichung, Taiwan, 2015, pp. 796–805, doi: 10.1109/COMPSAC.2015.117.

[16] D. Wang, P. M. Comar, and P.-N. Tan, "Crowdsourcing of network data," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Vancouver, BC, Canada, 2016, pp. 2204–2211, doi: 10.1109/IJCNN.2016.7727472.

[17] P. Welinder and P. Perona, "Online crowdsourcing: Rating annotators and obtaining cost-effective labels," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, San Francisco, CA, USA, 2010, pp. 25–32, doi: 10.1109/CVPRW.2010.5543189.

[18] M. S. Shahriar and M. S. Rahman, "Urban sensing and smart home energy optimisations: A machine learning approach," in *Proc. Int. Workshop Internet Things Towards Appl. (IoT App)*, Seoul, South Korea, 2015, pp. 19–22, doi: 10.1145/2820975.2820979.

[19] L. A. Hang-Yat and D. Wang, "Carrying my environment with me: A participatory-sensing approach to enhance thermal comfort," in *Proc. ACM Workshop Embedded Syst. Energy Efficient Build. (BuildSys)*, Roma, Italy, 2013, pp. 1–8, doi: 10.1145/2528282.2528286.

[20] C. Meurisch, K. Planz, D. Schäfer, and I. Schweizer, "Noisemap: Discussing scalability in participatory sensing," in *Proc. ACM Int. Workshop Sens. Big Data Min. (SenseMine)*, Roma, Italy, 2013, pp. 1–6, doi: 10.1145/2536714.2536720.

[21] M.-R. Ra, B. Liu, T. F. L. Porta, and R. Govindan, "Medusa: A programming framework for crowd-sensing applications," in *Proc. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, 2012, pp. 337–350, doi: 10.1145/2307636.2307668.

[22] M. Elhamshary, M. Youssef, A. Uchiyama, H. Yamaguchi, and T. Higashino, "TransitLabel: A crowd-sensing system for automatic labeling of transit stations semantics," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Singapore, 2016, pp. 193–206, doi: 10.1145/2906388.2906395.

[23] T. Franke, P. Lukowicz, M. Wirz, and E. Mitleton-Kelly, "Participatory sensing and crowd management in public spaces," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Taipei, Taiwan, 2016, pp. 485–486, doi: 10.1145/2462456.2465739.

[24] T. Yan, V. Kumar, and D. Ganesan, "CrowdSearch: Exploiting crowds for accurate real-time image search on mobile phones," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, San Francisco, CA, USA, 2010, pp. 77–90, doi: 10.1145/1814433.1814443.

[25] Y. Agarwal and M. Hall, "ProtectMyPrivacy: Detecting and mitigating privacy leaks on IOS devices using crowdsourcing," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Taipei, Taiwan, 2013, pp. 97–110, doi: 10.1145/2462456.2464460.

[26] S. Singla and A. Misra, "Indoor location error-detection via crowdsourced multi-dimensional mobile data," in *Proc. ACM Workshop Mobile Data (MobiData)*, Singapore, 2016, pp. 19–24, doi: 10.1145/2935755.2935762.

[27] D. Estrin *et al.*, "Participatory sensing: Applications and architecture [Internet predictions]," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 12–42, Jan./Feb. 2010, doi: 10.1109/MIC.2010.12.

[28] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma, "PRISM: Platform for remote sensing using smartphones," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, San Francisco, CA, USA, 2010, pp. 63–76, doi: 10.1145/1814433.1814442.

[29] A. Kittur, E. H. Chi, and B. Suh, "Crowdsourcing user studies with mechanical Turk," in *Proc. ACM SIGCHI Conf. Human Factors Comput. Syst.*, Florence, Italy, 2008, pp. 453–456, doi: 10.1145/1357054.135712.

[30] P. Jain, J. Manweiler, A. Acharya, and K. Beaty, "FOCUS: Clustering crowdsourced videos by line-of-sight," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Rome, Italy, 2013, pp. 1–14, doi: 10.1145/2517351.2517356.

[31] S. Chen, M. Li, K. Ren, X. Fu, and C. Qiao, "Rise of the indoor crowd: Reconstruction of building interior view via mobile crowdsourcing," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Seoul, South Korea, 2015, pp. 59–71, doi: 10.1145/2809695.2809702.

[32] H. Xiong, D. Zhang, L. Wang, J. P. Gibson, and J. Zhu, "EEMC: Enabling energy-efficient mobile crowdsensing with anonymous participants," *ACM Trans. Intell. Syst. Technol.*, vol. 6, no. 3, pp. 1–26, Apr. 2015, doi: 10.1145/2644827.

[33] N. D. Lane *et al.*, "Piggyback crowdsensing (PCS): Energy efficient crowdsourcing of mobile sensor data by exploiting smartphone app opportunities," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Rome, Italy, 2013, pp. 1–14, doi: 10.1145/2517351.2517372.

[34] K. L. Huang, S. S. Kanhere, and W. Hu, "A privacy-preserving reputation system for participatory sensing," in *Proc. Conf. Local Comput. Netw. (LCN)*, 2012, pp. 12–18, doi: 10.1109/LCN.2012.6423585.

[35] I. Krontiris and T. Dimitriou, "Privacy-respecting discovery of data providers in crowd-sensing applications," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Cambridge, MA, USA, 2013, pp. 249–257, doi: 10.1109/DCOSS.2013.31.

[36] J. Ren, Y. Zhang, K. Zhang and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: Challenges and solutions," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 98–105, Mar. 2015, doi: 10.1109/MCOM.2015.7060488.

[37] J. Sun, "An incentive scheme based on heterogeneous belief values for crowd sensing in mobile social networks," in *Proc. IEEE Conf. Glob. Commun. (GLOBECOM)*, Atlanta, GA, USA, 2013, pp. 1717–1722, doi: 10.1109/GLOCOM.2013.6831321.

[38] J. An, X. Gui, Z. Wang, J. Yang, and X. He, "A crowdsourcing assignment model based on mobile crowd sensing in the Internet of Things," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 358–369, Oct. 2015, doi: 10.1109/JIOT.2015.2415035.

[39] H. Amintoosi and S. S. Kanhere, "Privacy-aware trust-based recruitment in social participatory sensing," in *Proc. Conf. Mobile Ubiquitous Syst. Comput. Netw. Services (MobiQuitous)*, Tokyo, Japan, 2013, pp. 262–275, doi: 10.1007/978-3-319-11569-6_21.

[40] H. Amintoosi and S. S. Kanhere, "A trust-based recruitment framework for multi-hop social participatory sensing," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, Cambridge, MA, USA, 2013, pp. 266–273, doi: 10.1109/DCOSS.2013.29.

[41] T. Luo, S. S. Kanhere, S. K. Das, and H.-P. Tan, "Incentive mechanism design for heterogeneous crowdsourcing using all-pay contests," *IEEE Trans. Mobile Comput.*, vol. 15, no. 9, pp. 2234–2246, Sep. 2016, doi: 10.1109/TMC.2015.2485978.

[42] H. Amintoosi, S. S. Kanhere, and M. Allahbakhsh, "Trust-based privacy-aware worker selection in social participatory sensing," *J. Inf. Security Appl.*, vol. 20, pp. 11–25, Feb. 2015, doi: 10.1016/j.jisa.2014.10.003.

[43] Y. Wu, Y. Wu, H. Peng, H. Chen, and C. Li, "MagiCrowd: A crowd based incentive for location-aware crowd sensing," in *Proc. IEEE Conf. Wireless Commun. Netw. (WCNC)*, Doha, Qatar, 2016, pp. 1–6, doi: 10.1109/WCNC.2016.7565026.

[44] C. Tanas, S. Delgado-Segura, and J. Herrera-Joancomartí, "An integrated reward and reputation mechanism for MCS preserving users' privacy," in *Proc. Int. Workshop Data Privacy Manag. (DPM)*, 2015, pp. 83–99, doi: 10.1007/978-3-319-29883-2_6.

[45] Y. Wen *et al.*, "Quality-driven auction-based incentive mechanism for mobile crowd sensing," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4203–4214, Sep. 2015, doi: 10.1109/TVT.2014.2363842.

[46] D. Zhao, X.-Y. Li, and H. Ma, "Budget-feasible online incentive mechanisms for crowdsourcing tasks truthfully," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 647–661, Apr. 2016, doi: 10.1109/TNET.2014.2379281.

[47] S. Luo, Y. Sun, Z. Wen, and Y. Ji, "C2: Truthful incentive mechanism for multiple cooperative tasks in mobile cloud," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6, doi: 10.1109/ICC.2016.7511052.

[48] Z. Feng *et al.*, "Towards truthful mechanisms for mobile crowdsourcing with dynamic smartphones," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Madrid, Spain, 2014, pp. 11–20, doi: 10.1109/ICDCS.2014.10.

[49] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Nara, Japan, 2016, pp. 344–353, doi: 10.1109/ICDCS.2016.50.

[50] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing," *IEEE J. Internet Things*, vol. 2, no. 6, pp. 562–572, Dec. 2015, doi: 10.1109/JIOT.2015.2441031.

[51] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "You better be honest: Discouraging free-riding and false-reporting in mobile crowdsourcing," in *Proc. IEEE Conf. Glob. Commun. (Globecom)*, Austin, TX, USA, 2014, pp. 4971–4976, doi: 10.1109/GLOCOM.2014.7037593.

[52] T. Luo, S. K. Das, H. P. Tan, and L. Xia, "Incentive mechanism design for crowdsourcing: An all-pay auction approach," *ACM Trans. Intell. Syst. Technol.*, vol. 7, no. 3, pp. 1–35, Apr. 2016, doi: 10.1145/2837029.

[53] Y. Zhang, H. Zhang, S. Tang, and S. Zhong, "Designing secure and dependable mobile sensing mechanisms with revenue guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 100–113, Jan. 2016, doi: 10.1109/TIFS.2015.2478739.

[54] J. Sun and H. Ma, "Privacy-preserving verifiable incentive mechanism for online crowdsourcing markets," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Shanghai, China, 2014, pp. 1–8, doi: 10.1109/ICCCN.2014.6911794.

[55] Y. Wang *et al.*, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Comput. Netw.*, vol. 102, pp. 157–171, Jun. 2016, doi: 10.1016/j.comnet.2016.03.016.

[56] T. Dimitriou and I. Krontiris, "Privacy-respecting auctions as incentive mechanisms in mobile crowd sensing," in *Proc. Int. Conf. Inf. Security Theory Pract. (IFIP)*, 2015, pp. 20–35, doi: 10.1007/978-3-319-24018-3_2.

[57] J. Mineraud, F. Lancerin, S. Balasubramaniam, M. Conti, and S. Tarkoma, "You are airing too much: Assessing the privacy of users in crowdsourcing environmental data," in *Proc. IEEE Conf. Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 523–530, doi: 10.1109/Trustcom.2015.415.

[58] L. Kazemi and C. Shahabi, "TAPAS: Trustworthy privacy-aware participatory sensing," *Knowl. Inf. Syst.*, vol. 37, no. 1, pp. 105–128, Oct. 2013, doi: 10.1007/s10115-012-0573-y.

[59] L. Pournajaf, L. Xiong, and V. Sunderam, "Dynamic data driven crowd sensing task assignment," *Proc. Comput. Sci.*, vol. 29, pp. 1314–1323, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914002956?via%3Dihub, doi: 10.1016/j.procs.2014.05.118.

[60] L. Pournajaf, L. Xiong, V. Sunderam, and S. Goryczka, "Spatial task assignment for crowd sensing with cloaked locations," in *Proc. IEEE Int. Conf. Mobile Data Manag. (MDM)*, vol. 1. Brisbane, QLD, Australia, 2014, pp. 73–82, doi: 10.1109/MDM.2014.15.

[61] 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, doi: 10.14778/2732951.2732966.

[62] L. Zhang, X. Lu, P. Xiong, and T. Zhu, "A differentially private method for reward-based spatial crowdsourcing," in *Proc. Int. Conf. Appl. Tech. Inf. Security (ATIS)*, 2015, pp. 153–164, doi: 10.1007/978-3-662-48683-2_14.

[63] D. Christin, F. Engelmann, and M. Hollick, "Usable privacy for mobile sensing applications," in *Proc. Int. Workshop Inf. Security Theory Pract. (WISTP)*, 2014, pp. 92–107, doi: 10.1007/978-3-662-43826-8_7.

[64] Y. Gong, L. Wei, Y. Guo, C. Zhang, and Y. Fang, "Optimal task recommendation for mobile crowdsourcing with privacy control," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 745–756, Oct. 2016, doi: 10.1109/JIOT.2015.2512282.

[65] Y. Gong, Y. Guo, and Y. Fang, "A privacy-preserving task recommendation framework for mobile crowdsourcing," in *Proc. IEEE Conf. Glob. Commun. Conf. (Globecom)*, Austin, TX, USA, 2014, pp. 588–593, doi: 10.1109/GLOCOM.2014.7036871.

[66] B. Ye, Y. Wang, and L. Liu, "Crowd trust: A context-aware trust model for worker selection in crowdsourcing environments," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, New York, NY, USA, 2015, pp. 121–128, doi: 10.1109/ICWS.2015.26.

[67] F. Günther, M. Manulis, and A. Peter, "Privacy-enhanced participatory sensing with collusion resistance and data aggregation," in *Proc. Conf. Cryptol. Netw. Security (CANS)*, Heraklion, Greece, 2014, pp. 321–336, doi: 10.1007/978-3-319-12280-9_21.

[68] J. Chen, H. Ma, and D. Zhao, "Private data aggregation with integrity assurance and fault tolerance for mobile crowd-sensing," *Wireless Netw.*, vol. 23, no. 1, pp. 131–144, Jan. 2017, doi: 10.1007/s11276-015-1120-z.

[69] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing," in *Proc. Annu. IEEE Conf. Comput. Commun. (INFOCOM)*, San Francisco, CA, USA, 2016, pp. 1–9, doi: 10.1109/INFOCOM.2016.7524547.

[70] Z. Xie, L. Hu, F. Wang, J. Li, and K. Zhao, "PEMM: A privacy-aware data aggregation solution for mobile sensing networks," in *Proc. Int. Symp. Intell. Comput. Appl. (ISICA)*, 2015, pp. 474–482, doi: 10.1007/978-981-10-0356-1_50.

[71] S. Blasco, J. Bustos-Jimenez, G. Font, A. Hevia, and M. G. Prato, "A three-layer approach for protecting smart-citizens privacy in crowdsensing projects," in *Proc. Int. Conf. Chilean Comput. Sci. Soc. (SCCC)*, Santiago, Chile, 2015, pp. 1–5, doi: 10.1109/SCCC.2015.7416585.

[72] S. Wang *et al.*, "Personalized privacy-preserving data aggregation for histogram estimation," in *Proc. IEEE Conf. Glob. Commun. (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1–6, doi: 10.1109/GLOCOM.2015.7417364.

[73] L. R. Varshney, A. Vempaty, and P. K. Varshney, "Assuring privacy and reliability in crowdsourcing with coding," in *Proc. Inf. Theory Appl. Workshop (ITA)*, San Diego, CA, USA, 2014, pp. 1–6, doi: 10.1109/ITA.2014.6804213.

[74] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "INCEPTION: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proc. Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, vol. 16. pp. 341–350, 2016, doi: 10.1145/2942358.2942375.

[75] C. Miao *et al.*, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Seoul, South Korea, 2015, pp. 183–196, doi: 10.1145/2809695.2809719.

[76] R. W. Ouyang, M. Srivastava, A. Toniolo, and T. J. Norman, "Truth discovery in crowdsourced detection of spatial events," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 4, pp. 1047–1060, Apr. 2016, doi: 10.1109/TKDE.2015.2504928.

[77] A. Kurve, D. J. Miller, and G. Kesidis, "Multicategory crowdsourcing accounting for variable task difficulty, worker skill, and worker intention," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 3, pp. 794–809, Mar. 2015, doi: 10.1109/TKDE.2014.2327026.

[78] B. Kantarci and H. T. Mouftah, "Trustworthy crowdsourcing via mobile social networks," in *Proc. IEEE Conf. Glob. Commun. Conf. (GLOBECOM)*, Austin, TX, USA, 2014, pp. 2905–2910, doi: 10.1109/GLOCOM.2014.7037249.

[79] B. Kantarci and H. T. Mouftah, "Mobility-aware trustworthy crowdsourcing in cloud-centric Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Funchal, Portugal, 2014, pp. 1–6, doi: 10.1109/ISCC.2014.6912581.

[80] L. R. Varshney, "Privacy and reliability in crowdsourcing service delivery," in *Proc. Annu. Conf. SRII Glob. (SRII)*, 2012, pp. 55–60, doi: 10.1109/SRII.2012.17.

[81] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment framework for participatory sensing data collections," in *Proc. Int. Conf. Pervasive Comput. (PERVASIVE)*, Newcastle, U.K., 2012, pp. 138–155, doi: 10.1007/978-3-642-12654-3_9.

[82] R. W. Ouyang, L. M. Kaplan, A. Toniolo, M. Srivastava, and T. J. Norman, "Aggregating crowdsourced quantitative claims: Additive and multiplicative models," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 7, pp. 1621–1634, Jul. 2016, doi: 10.1109/TKDE.2016.2535383.

[83] J. Zhang, V. S. Sheng, J. Wu, and X. Wu, "Multi-class ground truth inference in crowdsourcing with clustering," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 4, pp. 1080–1085, Apr. 2016, doi: 10.1109/TKDE.2015.2504974.

[84] C. Prandi, S. Ferretti, S. Mirri, and P. Salomoni, "A trustworthiness model for crowdsourced and crowdsensed data," in *Proc. Conf. Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 1261–1266, doi: 10.1109/Trustcom.2015.515.

[85] G. Drosatos, P. S. Efraimidis, I. N. Athanasiadis, E. D'Hondt, and M. Stevens, "A privacy-preserving cloud computing system for creating participatory noise maps," in *Proc. IEEE Annu. Conf. Comput. Softw. Appl. (COMPSAC)*, Izmir, Turkey, 2012, pp. 581–586, doi: 10.1109/COMPSAC.2012.78.

[86] D. Wang, T. Abdelzaher, L. Kaplan, and C. C. Aggarwal, "Recursive fact-finding: A streaming approach to truth estimation in crowdsourcing applications," in *Proc. Conf. Distrib. Comput. Syst. (ICDCS)*, Philadelphia, PA, USA, 2013, pp. 530–539, doi: 10.1109/ICDCS.2013.54.

[87] A. Etuk, T. J. Norman, C. Bisdikian, and M. Srivatsa, "TAF: A trust assessment framework for inferencing with uncertain streaming information," in *Proc. IEEE Conf. Pervasive Comput. Commun. Workshops (PERCOM)*, San Diego, CA, USA, 2013, pp. 475–480, doi: 10.1109/PerComW.2013.6529544.

[88] C. Meng *et al.*, "Truth discovery on crowd sensing of correlated entities," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Seoul, South Korea, 2015, pp. 169–182, doi: 10.1109/PerComW.2013.6529544.

[89] C. Meng, H. Xiao, L. Su, and Y. Cheng, "Tackling the redundancy and sparsity in crowd sensing application," in *Proc. ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Stanford, CA, USA, 2016, pp. 150–163, doi: 10.1145/2809695.2809715.

[90] J. Hamm, A. C. Champion, G. Chen, M. Belkin, and D. Xuan, "Crowd-ML: A privacy-preserving learning framework for a crowd of smart devices," in *Proc. Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Columbus, OH, USA, 2015, pp. 11–20, doi: 10.1109/ICDCS.2015.10.

[91] D. Ye, Y. Mei, Y. Shang, J. Zhu, and K. Ouyang, "Mobile crowdsensing context aware based fine-grained access control mode," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13977–13993, Nov. 2016, doi: 10.1007/s11042-015-2693-3.

[92] O. Folorunso and O. A. Mustapha, "A fuzzy expert system to trust-based access control in crowdsourcing environments," *Appl. Comput. Informat.*, vol. 11, no. 2, pp. 116–129, Jul. 2015, doi: 10.1016/j.aci.2014.07.001.

[93] J. Chang *et al.*, "TrustForge: Flexible access control for collaborative crowd-sourced environment," in *Proc. Annu. Int. Conf. Privacy Security Trust (PST)*, Tarragona, Spain, 2013, pp. 291–300, doi: 10.1109/PST.2013.6596065.

[94] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava, "SensorSafe: A framework for privacy-preserving management of personal sensory information," in *Proc. Workshop Secure Data Manag. (SDM)*, Seattle, WA, USA, 2011, pp. 85–100, doi: 10.1007/978-3-642-23556-6_6.

[95] J. Zhou, Z. Cao, and X. Dong, "Secure and efficient fine-grained multiple file sharing in cloud-assisted crowd sensing networks," *Peer Peer Netw. Appl.*, vol. 9, no. 4, pp. 774–794, Jul. 2016, doi: 10.1007/s12083-016-0449-0.

[96] T. Dimitriou, I. Krontiris, and A. Sabouri, "PEPPeR: A querier's privacy enhancing protocol for participatory sensing," in *Proc. Int. Conf. Security Privacy Mobile Inf. Commun. Syst. (MobiSec)*, 2012, pp. 93–106, doi: 10.1007/978-3-642-33392-7_11.

[97] I. Boutsis and V. Kalogeraki, "Privacy preservation for participatory sensing data," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2013, pp. 103–113, doi: 10.1109/PerCom.2013.6526720.

[98] H. Amintoosi and S. S. Kanhere, "A reputation framework for social participatory sensing systems," *Mobile Netw. Appl.*, vol. 19, no. 1, pp. 88–100, Feb. 2014, doi: 10.1007/s11036-013-0455-x.

[99] H. Amintoosi and S. S. Kanhere, "A trust framework for social participatory sensing systems," in *Proc. Conf. Mobile Ubiquitous Syst. Comput. Netw. Services (MobiQuitous)*, 2013, pp. 237–249, doi: 10.1007/978-3-642-40238-8_20.

[100] C. Wu, T. Luo, F. Wu, and G. Chen, "EndorTrust: An endorsement-based reputation system for trustworthy and heterogeneous crowdsourcing," in *Proc. IEEE Conf. Glob. Commun. (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1–6, doi: 10.1109/GLOCOM.2015.7417352.

[101] A. Manzoor, M. Asplund, M. Bouroche, S. Clarke, and V. Cahill, "Trust evaluation for participatory sensing," in *Proc. Conf. Mobile Ubiquitous Syst. Comput. Netw. Services (MobiQuitous)*, 2013, pp. 176–187, doi: 10.1007/978-3-642-40238-8_15.

[102] S. Vaya, "Robust reputation mechanisms for achieving fair compensation and quality assurance in crowdcomputing," in *Proc. IEEE Int. Conf. Soc. Informat. (SocialInformatics)*, 2012, pp. 228–235, doi: 10.1109/SocialInformatics.2012.50.

[103] D. Ceolin *et al.*, "Combining user reputation and provenance analysis for trust assessment," *J. Data Inf. Qual.*, vol. 7, nos. 1–2, pp. 1–28, Jan. 2016, doi: 10.1145/2818382.

[104] X. O. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "ARTSense: Anonymous reputation and trust in participatory sensing," in *Proc. IEEE Int. Conf. Comput. (INFOCOM)*, 2013, pp. 2517–2525, doi: 10.1109/INFCOM.2013.6567058.

[105] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervasive Mobile Comput.*, vol. 9, no. 3, pp. 353–371, Jun. 2013, doi: 10.1016/j.pmcj.2013.01.003.

[106] K. L. Huang, S. S. Kanhere, and W. Hu, "Are you contributing trustworthy data? The case for a reputation system in participatory sensing," in *Proc. ACM Int. Conf. Model. Anal. Simulat. Wireless Mobile Syst. (MSWIM)*, 2010, pp. 14–22, doi: 10.1145/1868521.1868526.

[107] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "SACRM: Social aware crowdsourcing with reputation management in mobile sensing," *Comput. Commun.*, vol. 65, pp. 55–65, Jul. 2015, doi: 10.1016/j.comcom.2015.01.022.

[108] S. Wu, X. Wang, S. Wang, Z. Zhang, and A. K. H. Tung, "K-anonymity for crowdsourcing database," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2207–2221, Sep. 2014, doi: 10.1109/TKDE.2013.93.

[109] K. Dua, N. Bulusu, W. Feng, and W. Hu, "Combating software and Sybil attacks to data integrity in crowd-sourced embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 13, no. 5, pp. 1–19, Nov. 2014, doi: 10.1145/2629338.

[110] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "Security, privacy, and incentive provision for mobile crowd sensing systems," *J. Internet Things*, vol. 3, no. 5, pp. 839–853, Oct. 2016, doi: 10.1109/JIOT.2016.2560768.

[111] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2015, doi: 10.1109/TMC.2014.2352253.

[112] E. Pournaras, I. Moise, and D. Helbing, "Privacy-preserving ubiquitous social mining via modular and compositional virtual sensors," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Gwangju, South Korea, 2015, pp. 332–338, doi: 10.1109/AINA.2015.203.

[113] C. Sauerwein, M. Gander, M. Felderer, and R. Breu, "A systematic literature review of crowdsourcing-based research in information security," in *Proc. IEEE Symp. Service Orient. Syst. Eng. (SOSE)*, Oxford, U.K., 2017, pp. 364–371, doi: 10.1109/SOSE.2016.67.

[114] G. Wang *et al.*, "Defending against Sybil devices in crowdsourced mapping services," in *Proc. Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, 2016, pp. 179–191, doi: 10.1145/2906388.2906420.

[115] L. Pournajaf, L. Xiong, D. A. Garcia-Ulloa, and V. Sunderam, "A survey on privacy in mobile crowd sensing task management," Dept. Math. Comput. Sci. and Dept. Biomed. Informat., Emory Univ., Atlanta, GA, USA, Tech. Rep. TR-2014-002, pp. 1–5, 2014.

[116] H. Mousa *et al.*, "Trust management and reputation systems in mobile participatory sensing applications: A survey," *Comput. Netw.*, vol. 90, pp. 49–73, Oct. 2015, doi: 10.1016/j.comnet.2015.07.011.

[117] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *J. Syst. Softw.*, vol. 84, no. 11, pp. 1928–1946, Nov. 2011, doi: 10.1016/j.jss.2011.06.073.

[118] D. Christin, "Privacy in mobile participatory sensing: Current trends and future challenges," *J. Syst. Softw.*, vol. 116, pp. 57–68, Jun. 2016, doi: 10.1016/j.jss.2015.03.067.

[119] Y. Zhao and Q. Han, "Spatial crowdsourcing: Current state and future directions," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 102–107, Jul. 2016, doi: 10.1109/MCOM.2016.7509386.

[120] D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in mobile crowd sensing," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 28–34, Feb. 2015, doi: 10.1109/MWC.2015.7054716.

[121] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable set operation in big data for cloud-assisted mobile crowdsourcing," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 572–582, Apr. 2017, doi: 10.1109/JIOT.2016.2585592.

[122] J. Ni, K. Zhang, X. Lin, Q. Xia, and X. S. Shen, "Privacy-preserving mobile crowdsensing for located-based applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, pp. 1–6, doi: 10.1109/ICC.2017.7997116.

[123] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017, doi: 10.1109/MCOM.2017.1600679.

[124] T. Zhou, Z. Cai, K. Wu, Y. Chen, and M. Xu, "FIDC: A framework for improving data credibility in mobile crowdsensing," *Comput. Netw.*, vol. 120, pp. 157–169, Apr. 2017, doi: 10.1016/j.comnet.2017.04.015.

[125] C. Huang, R. Lu, and H. Zhu, "Privacy-friendly spatial crowdsourcing in vehicular networks," *J. Commun. Inf. Netw.*, vol. 2, no. 2, pp. 59–74, 2017, doi: 10.1007/s41650-017-0017-7.

[126] X. Duan, C. Zhao, S. He, P. Cheng, and J. Zhang, "Distributed algorithms to compute Walrasian equilibrium in mobile crowdsensing," *IEEE Trans. Ind. Electron.*, vol. 64, no. 5, pp. 4048–4057, May 2017, doi: 10.1109/TIE.2016.2645138.

[127] T. Li *et al.*, "Scalable privacy-preserving participant selection in mobile crowd sensing," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2017, pp. 59–68, doi: 10.1109/PERCOM.2017.791785.

[128] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

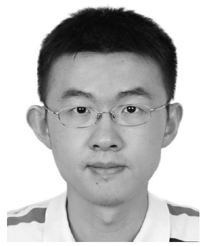
Wei Feng received the B.Sc. degree in telecommunications engineering from Xidian University, Xi'an, China, in 2014, where he is currently pursuing the Ph.D. degree in information security.

His current research interests include information security, privacy preservation, and trust management in social networking and mobile crowdsourcing.

Zheng Yan (M'06–SM'14) received the B.Eng. degree in electrical engineering and M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science and the Doctor of Science in Technology degrees in electrical engineering from the Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007, respectively.

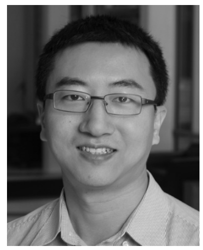
She is currently a Professor with Xidian University, Xi'an, and a Visiting Professor with Aalto University, Espoo, Finland. She has authored over 170 publications and 2 books. She holds over 60 patents and patent applications. Her current research interests include trust, security and privacy, social networking, cloud computing, networking systems, and data mining.

Prof. Yan serves as an Organization and Program Committee member for numerous international conferences and workshops. She is also an Associate Editor or a Guest Editor of several journals such as *Information Sciences*, *ACM TOMM*, *Information Fusion*, the IEEE SYSTEMS JOURNAL, the IEEE INTERNET OF THINGS JOURNAL, and IEEE ACCESS.



Hengrun Zhang received the B.Sc. degree from the East China University of Science and Technology, Shanghai, China, in 2012, and the M.S. degree from Shanghai Jiao Tong University, Shanghai, in 2012.

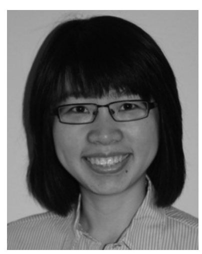
He is currently a Research Assistant with the Department of Computer Science and the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. His current research interests include mobile crowdsourcing security, machine learning and data mining, and computer vision.



Kai Zeng (S'05–M'08) received the Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI), Worcester, MA, USA, in 2008.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, the Department of Computer Science, and the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. From 2008 to 2011, he was a Post-Doctoral Scholar with the Department of Computer Science, University of California at Davis (UCD), Davis, CA, USA. From 2011 to 2014, he was an Assistant Professor with the Department of Computer and Information Science, University of Michigan–Dearborn, Dearborn, MI, USA. His current research interests include cyber-physical system security and privacy, physical layer security, network forensics, and cognitive radio networks.

Dr. Zeng was a recipient of the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008, the Excellence in Post-Doctoral Research Award from UCD in 2011, and the U.S. National Science Foundation Faculty Early Career Development Award in 2012. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.



Yu Xiao received the bachelor's and master's degrees in computer science from the Beijing University of Posts and Telecommunications, Beijing, China, and the Doctoral degree in computer science from Aalto University, Espoo, Finland, in 2012.

She is currently an Assistant Professor with the Department of Communications and Networking, Aalto University. Her current research interests include energy-efficient mobile computing, ubiquitous cloud computing, and mobile crowdsensing.

Y. Thomas Hou (S'90–M'91–SM'04–F'14) received the Ph.D. degree from the New York University Tandon School of Engineering, Brooklyn, NY, USA, in 1998.

He is a Bradley Distinguished Professor in electrical and computer engineering with the Virginia Polytechnic Institute and State University, Blacksburg, VA, USA. From 1997 to 2002, he was a Researcher with the Fujitsu Laboratories of America, Sunnyvale, CA, USA. He authored two textbooks entitled *Cognitive Radio Communications and Networks: Principles and Practices* (Academic/Elsevier, 2009) and *Applied Optimization Methods for Wireless Networks* (Cambridge Univ. Press, 2014). He holds five U.S. patents. His current research interests include develop innovative solutions to complex cross-layer optimization problems in wireless networks and exploring new performance limits at the network layer by exploiting advances at the physical layer.

Prof. Hou was a recipient of five Best Paper Awards of the IEEE and two Paper Awards of the ACM. His first book has been selected as one of the Best Readings on Cognitive Radio by the IEEE Communications Society. He is the Steering Committee Chair of the IEEE INFOCOM Conference. He is a member of the Board of Governors and a Distinguished Lecturer of the IEEE Communications Society.