International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-4, Issue-6, June 2018 Pages 71-76

A Survey on Security, Privacy and Trust in Mobile Crowdsourcing

Manali Bhavsar, Snehil Dahima

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 (WSN), 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— **MCS,Mobile Crowdsourcing, WSN, Wireless Sensor Networks.**

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 allow them to collect various types of data such as image/voice/video, location, and ambient information. Many 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 involves activities that take place on smartphones or mobile platforms that are frequently characterized by GPS technology. This allows for real-time data gathering and gives projects greater reach and accessibility.

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.

A 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.

Many MCS applications have been developed [1-31] and are used for environment monitoring [2, 4], infrastructure monitoring quality of-experience analysis [8, 9], surface perception [5], and public safety [7]. In parallel to MCS applications, there are some studies aiming at

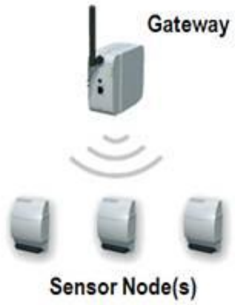
improving the energy-efficiency in MCS [32, 33]. For instance, Lane et al. [33] proposed Piggyback Crowd Sensing (PCS), which tried to reduce the overhead of data collection by exploiting Smartphone App Opportunities. [1, 2, 3]

Miss. Manali Bhavsar, MCA Sem VI, SIES College of Management Studies

Prof. Snehil Dahima, MCA/MBA, SIES College of Management Studies

II. LITERATURE REVIEW

- **OVERVIEW OF WSN (Wireless Sensor Network)**



A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes .The wireless protocol you select depends on your application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

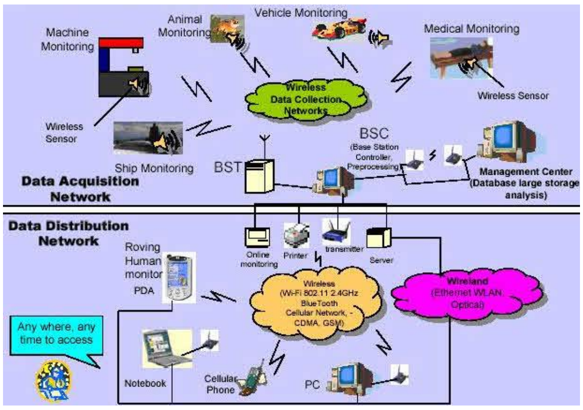
- **Potential Applications**

Engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include:

- Environmental monitoring of air, water, and soil
- Structural monitoring for buildings and bridges
- Industrial machine monitoring
- Process monitoring
- Asset tracking

- **WSN System Architecture**

WSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors).These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location as shown in the figure.


Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC (Base Station Controller, Preprocessing)
Management Center (Database large storage analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor
PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

- **<u>OVERVIEW OF MCS</u>**

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.

- 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.

- 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.

- **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.

III. METHODOLOGY

- **<u>System Architecture of MCS</u>**

There are three main parties in a MCS system, namely MCS Service Provider (SP), End user (EU) and MCS worker.

- **MCS Service Provider:**

MCS Service Provider 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. An MCS SP could be acted by a single or 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.

- **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.

- **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 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.

The diagram shows 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 a server that collects data from workers and delivers data processing is 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 [4]

- **Procedures of MCS Activities**

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.

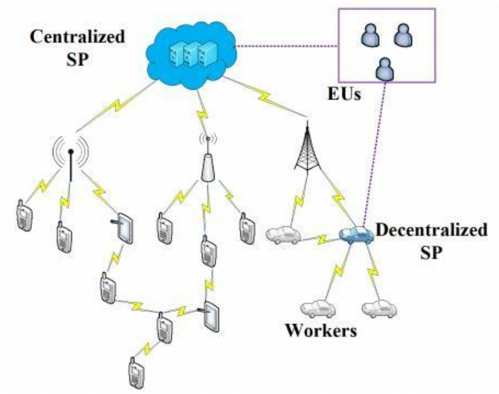
- **<u>Characteristics</u>**MCS integrates the concepts of mobility with crowdsourcing several special characteristics.
- **Openness:**

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.

- **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.

- **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.

- **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 data trust and worker trust. 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.

- **Requirements on Security, Privacy And Trust:**

Security means protecting collected data and MCS systems from unauthorized access, use, disclosure, disruption, modification, destruction, and 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.

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. In MCS, trust can be divided into worker trust, SP trust and collected data trust. [5]

- **Threat Analysis**

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.

- **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.

- **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 are 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. 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.

- **Threats to Task Privacy of End Users**

The privacy of a 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.

- **Trust Threats**

MCS faces trust threats in terms of worker trust and data trust, as well as SP trust. The worker trust 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 data trust. Therefore, the threats caused by both worker trust and data trust should be paid attention to. SP trust is another important issue. In the centralized server architecture, SP trust is similar to cloud computing trust. In terms of distributed server architecture or a fully distributed architecture, SP trust becomes a more challenging issue due to the nature of mobility, dynamicity and ubiquity of mobile SP in MCS. In Table 2, 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.

IV. RESULT

Table 2

		Attacks And Threats		
	Procedures	**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	False Personal Information, Impersonation Attack	Threat to Personal Information Privacy; Threat to Data Privacy	Threat to Worker Trust Threat to Data Trust

- **Requirements**

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

- **Confidentiality and Integrity (C/I):**

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. Therefore, it is necessary to guarantee data confidentiality and integrity to resist eavesdropping attack and protect data from being tampered.

- **Authenticity (Au):**

The MCS system should be able to verify that the data reports are from a valid worker that the sender declares. To provide authenticity, 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.

- **Worker Trust (WT):**

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

- **SP Trust (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.

- **Data Trust (DT):**

Data trust means that a 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.

- **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, personal information trust should be ensured to block false personal information uploading, and to encourage workers to upload real information.

- **Availability and Dependability (A/D):**

The MCS services should be available even under Denial-of-Service (DOS) or Distributed Denial-of Service (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.

- **Non-Repudiation (Nr):**

Usually, non-repudiation 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, non-repudiation 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. Non-repudiation can benefit to resist impersonate attack and the threats related to data transmission security, and help in maintaining the normal functions of the MCS system.

- **Revocation (Re):**

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 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

- **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.

- **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 access control 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.

DIFFERENCE BETWEEN MCS AND WSN

MCS has a number of advantages over traditional Wireless Sensor Networks (WSN).

1) 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.

2) The sensing devices in MCS are mobile and can provide a wider coverage than WSN.

3) 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.

4) 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 self-organized manner in such scenarios.

V. FUTURE ENHANCEMENT

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 data trust is highly related to worker trust, the authentication on the worker trust with privacy preservation is also important.

Important as it is, current work 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.

We also 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.

REFERENCES

[1] C. Hu, P. Resnik, and B. B. Bederson, “Crowdsourced Monolingual Translation,” ACM Trans. Computing Human Interaction, vol. 21, no. 4, pp. 1-35, Aug. 2014, doi: /10.1145/2627751.

[2] C. Chen, Y. Huang, Y. Lou, C. Liu, L. Meng, Y. Sun, K. Bian, A. Huang, X. Duan, and B. Jiao, “Interactive Crowdsourcing to Spontaneous Reporting of Adverse Drug Reactions,” Proc. IEEE International Conf. Communications (ICC’14), pp. 4275-4280, 2014, 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. Sensing Networking, vol. 11, no. 4, pp. 1-27, July 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 Communications Magazine, 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. Application 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,” Proc. IEEE International Conf. Communications (ICC’14), pp. 227-232, 2014, doi: 10.1109/ICC.2014.6883323.

[7] B. Kantarci and H. T. Mouftah, “Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things,” J. Internet of Things, 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, “LIRISACCEDE: A Video Database for Affective Content Analysis,” IEEE Trans. Affective Computing, vol. 6, no. 1, pp. 43-55, Jan. 2015, doi: 10.1109/TAFFC.2015.2396531.

[10] M. Pouryazdan, B. Kantarci, T. Soyata and H. Song, “AnchorAssisted and Vote-Based Trustworthiness Assurance in Smart City Crowdsensing,” IEEE Access, vol. 4, pp. 529-541, Jan. 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 and Mobile Computing, vol. 20, pp. 1-12, July 2015, doi: 10.1016/j.pmcj.2014.12.007.

[12] Le. Tan, H. Fan, W. Rui, Z. Xu, S. Zhang, J. Xu, and K. Xing, “Mining Myself in the Community: Privacy Preserved Crowd Sensing and Computing,” Proc. International Conf. Wireless Algorithms, Systems, and Applications (WASA’16), pp. 272-282, 2016, 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,” Proc. IEEE International Conf. Acoustics, Speech and Signal Processing (ICASSP’15), pp. 5256-5260, 2015, doi: 10.1109/ICASSP.2015.7178974.

[14] T. Zhu, J. Behar, T. Papastylianou, and G. D. Clifford, “CrowdLabel: A Crowdsourcing Platform for Electrophysiology,” Proc. Conf. Computing in Cardiology (CINC’14), pp. 789-792, 2014.

[15] T. Kubota and M. Aritsugi, “How Many Ground Truths Should We Insert? Having Good Quality of Labeling Tasks in Crowdsourcing,” Proc. IEEE Conf. Computer Software and Applications Conference (COMPSAC’15), pp. 796-805, 2015, doi: 10.1109/COMPSAC.2015.117.

[16] D. Wang, P. M. Comar, and P. N. Tan, “Crowdsourcing of Network Data,” Proc. International Joint Conf. Neural Networks (IJCNN’16), pp. 2204-2211, 2016, doi: 10.1109/IJCNN.2016.7727472.

[17] P. Welinder and P. Perona, “Online Crowdsourcing: Rating Annotators and Obtaining Cost-Effective Labels,” Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition, Workshops (CVPRW’10), pp. 25-32, 2010, doi: 10.1109/CVPRW.2010.5543189.

[18] M. S. Shahriar and M. S. Rahman, “Urban Sensing and Smart Home Energy Optimizations: A Machine Learning Approach,” Proc. International Workshop on Internet of Things towards Applications (IoT-App’15), pp. 19-22, 2015, 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,” Proc. ACM Workshop on Embedded Systems for EnergyEfficient Buildings (BuildSys’13), pp. 1-8, 2013, doi: 10.1145/2528282.2528286.

[20] C. Meurisch, K. Planz, D. Schäfer, and I. Schweizer, “Noisemap: Discussing Scalability in Participatory Sensing,” Proc. ACM International Workshop on Sensing and Big Data Mining (SenseMine’13)

[21] M. R. Ra, B. Liu, T. F. La Porta, and R. Govindan, “Medusa: A Programming Framework for Crowd-Sensing Applications,” Proc. International Conf. Mobile Systems, Applications, and Services (MobiSys’12), pp. 337-350, 2012, 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,” Proc. Ann. International Conf. Mobile Systems, Applications, and Services (MobiSys’ 16), pp. 193-206, 2016, doi: 10.1145/2906388.2906395.

[23] T. Franke, P. Lukowicz, M. Wirz, and E. Mitleton-Kelly, “Participatory Sensing and Crowd Management in Public Spaces,” Proc. Ann. International Conf. Mobile Systems, Applications, and Services (MobiSys’ 16), pp. 485-486, 2016, 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,” Proc. Ann. International Conf. Mobile Systems, Applications, and Services (MobiSys’ 10), pp. 77-90, doi: 2010, 10.1145/1814433.1814443.

[25] Y. Agarwal and M. Hall, “ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on IOS Devices Using Crowdsourcing,” Proc. Ann. International Conf. Mobile Systems, Applications, and Services (MobiSys’ 13), pp. 97-110, 2013, doi: 10.1145/2462456.2464460.

[26] S. Singla and A. Misra, “Indoor Location Error-Detection via Crowdsourced Multi-Dimensional Mobile Data,” Proc. ACM Workshop on Mobile Data (MobiData’16), pp. 19-24, 2016, doi: 10.1145/2935755.2935762.

[27] D. Estrin, K. M. Chandy, R. M. Young, L. Smarr, A. Odlyzko, D. Clark, and Hölzle, “Participatory Sensing: Applications and Architecture,” IEEE Internet Computing, vol. 14, no. 1, pp. 12-42, 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,” Proc. Ann. International Conf. Mobile Systems, Applications, and Services (MobiSys’ 10), pp. 63-76, 2010, doi: 10.1145/1814433.1814442.

[29] A. Kittur, E. H. Chi, and B. Suh, “Crowdsourcing User Studies with Mechanical Turk,” Proc. ACM SIGCHI Conf. Human Factors in Computing Systems, pp. 453-456, 2008, doi: 10.1145/1357054.135712.

[30] P. Jain, J. Manweiler, A. Acharya, and K. Beaty, “FOCUS: Clustering Crowdsourced Videos by Line-Of-Sight,” Proc. ACM Conf. Embedded Networked Sensor Systems (Sen-Sys’13), pp. 1-14, 2013, 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,” Proc. ACM Conf. Embedded Networked Sensor Systems (SenSys’15), pp. 59-71, 2015, doi: 10.1145/2809695.2809702.