IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 2, 2020, accepted January 16, 2020, date of publication January 22, 2020, date of current version January 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968797

Simulation of Trust-Based Mechanism for Enhancing User Confidence in Mobile Crowdsensing Systems

DOROTHY MWONGELI KALUI[1,2], DEZHENG ZHANG[1], GEOFFREY MUCHIRI MUKETHA[3], AND JARED OKOYO ONSOMU[4]

[1]Department of Computer Science, University of Science and Technology Beijing, Beijing 100083, China
[2]Department of Computer Science, Meru University of Science and Technology, Meru 60200, Kenya
[3]Department of Computer Science, Muranga University of Technology, Muranga 10200, Kenya
[4]University of Nairobi, Nairobi 30197, Kenya

Corresponding author: Dorothy Mwongeli Kalui (dkalui@yahoo.com)

This work was supported in part by the National Research Fund (NRF), Kenya, Multidisciplinary Research, under Grant 2016/2017.

ABSTRACT With the rapid development of mobile technology and subsequent mass adoption of mobile devices, mobile crowdsensing (MCS) has gained a lot of research attention. In MCS systems, trust is a key focus in the overall improvement in the participant uptake of the sensing tasks. The trust-based scheme of MCS is studied to predict the damage level, the scores of quality-of-service (QoS), and the levels of quality-of-data (QoD) of MCS systems. Users can participate in MCS sensing based on trustworthy indicators that are related to user experience and system reputation, as well as the knowledge obtained about the MCS systems. This paper illustrates the establishment of user confidence during recruitment in MCS as it is very critical for the success of MCS systems and proposes a simulation trust-based mechanism (SiTBaM) approach. The level of MCS security is enhanced to protect the privacy of participants, so that participants can be assured that the MCS system they are working with during sensing moment is trustworthy. The application of SiTBaM in MCS is verified to yield better results as the simulations show that it offers higher QoS levels, QoD scores, as well as low damage levels in the presence of any task or many malicious users. These results were validated through comparisons with other schemes.

INDEX TERMS Mobile crowdsensing, quality-of-data, quality-of-service, security, trust-based scheme.

I. INTRODUCTION

Mobile crowdsensing (MCS) has attracted significant focus in the recent past making it an appealing paradigm in the user communication sensing systems. The MCS system is a human-driven Internet of Things (IoT) service empowering citizens to observe the phenomena of individual, community, or even societal value by sharing sensor data about their environment while on the move [1]. There is an emerging human-powered modern sensing paradigm that leverages millions of individual mobile devices to sense, collect, analyze urban data without the deployment of any large number of static sensors as sensing infrastructures thus making it low cost and of spatial-temporal coverage [2], and this fits the category of MCS systems. MCS relies on contributions from mobile devices (i.e. smartphones, tablets, iPads, and wearable devices) [3] of a large number of users or crowd. Smartphones, tablets, iPads, and wearable devices are equipped with a rich set of sensors and deployed widely making them an excellent source of information. This new paradigm is more scalable and cost-effective than deploying static wireless sensor networks for dense-sensing coverage across large geographical areas [4]. Basically, MCS applications focus on community sensing tasks for large-scale phenomena that cannot easily be measured by a single individual. Rather, these phenomena can only be measured accurately when data are aggregated spatiotemporally from many individuals [5].

MCS system is different from conventional sensing solutions because it is powered using specialized networks of sensors aimed at leveraging human intelligence to collect, process, and aggregate sensing data using individuals' mobile devices (e.g., using a camera to capture a specific target),

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

so as to realize a higher quality and more efficient sensing solution [6]. The intelligence of humans together with the mobility aspects will guarantee a larger coverage and better context awareness if compared to the traditional sensing networks. However, the participants may be reluctant to share data that they deem to be of sensitive nature due to privacy concerns. Mobile crowdsensing is a new sensing paradigm that incorporates built-in sensors of mobile devices and human intelligence to monitor, share, analyze big and heterogeneous data about diverse phenomena [7]. A typical MCS system consists of a cloud-based platform and a large number of mobile devices or more commonly, the smartphone users, where the platform works as a sensing service buyer who posts the required sensing information and recruits a set of mobile device users to provide sensing services or to participate in the sensing campaign [8]. When the participant is once selected by the platform, he starts to collect the required data and sends it back to the requesting platform. The requester initiates a crowdsensing application that usually needs to have monetary investment so the inferred truths can be the data provided by mobile crowdsensing is used to design a variety of applications according to individual or group activities to model their behaviour and predict possible solutions for different patterns.

MCS technology has attracted much attention since this technology can perform sensing jobs that individual users cannot cope up with. In the case of participatory crowdsensing users, they can collude with each other to mislead the system by sending fake information since they own and control the devices used for MCS as these users may have unknown intentions, varied capabilities and unpredictable reliability which leads to untrustworthy data [9]. The participants or mobile users are registered as candidate workers to collect and contribute data through their sensing devices [10]. When a new task arrives, the MCS server selects some workers to complete these tasks but results in some issues in task allocation since the various participants possess diverse qualities on handling different tasks, hindering efficiency as it solely depends on the location information to calculate the distance between tasks and workers. If large distance exists between the target location of a task and the participant, then there will be greater rewards for completing the task unlike when the distance is short. In [11], it is argued that many participants are usually reluctant to participate in MCS campaigns either because of fear of their privacy, or because of resource (e.g. smartphone battery, and memory) consumption, thus making many researchers rely on voluntary participants.

In the case of large-scale MCS deployments, massive computational resources are required for device management and real-time data processing. Despite this challenge of massive resource requirements, large-scale and centralized MCS introduces other problems including

- generates significant load on mobile network
- creates increased traffic to cloud servers running MCS services,
- high computational cost, associated with real-time usage scenarios, due to a large number of devices participating in MCS tasks with frequently changing context,
- increased latency of data and information propagation, which is critical for real-time usage scenarios, and
- a threat to user privacy since all user traces are collected in a centralized manner.

The mobile edge technology is designed to enable third parties to run their services and applications at the edge of the mobile networks so that they can reduce these problems.

MCS is gaining a lot of familiarity in this era of mobile technology. According to Wikipedia, mobile crowdsensing is a mobile data-gathering technology where a large group of individuals who have mobile devices capable of sensing and computing collectively at the same time can share data and extract information to measure, map, analyze, estimate, or infer any processes of their common interest. This technique can also be summarized to mean crowdsourcing of sensor data from mobile devices which can be largely dispersed from each other. A number of individuals, forming the crowd, is committed to performing observations of real-world phenomena of common interest through the use of mobile phones, given their capacity to sense the environment and other phenomena in the community (e.g. finding the total number of people in a restaurant, or in a cinema hall given their GPS position) [12].

Currently, smart mobile devices are becoming increasingly popular everywhere and are equipped with very powerful sensors that have been pervasively applied in crowdsensing as effective tools to solve large-scale sensing tasks in urban areas. The group owner (GO) performs the coordination work by establishing contracts with mobile user devices to specify the expected results and their corresponding incentive payments [13]. These incentives can take various forms i.e. presence/location-aware, behavioural-aware, flat incentive, mobility-aware, and mixed incentive [14]. The task requesters can allocate sensing tasks to the mobile nodes through a crowdsensing platform, eliminating the cost of deploying and maintaining large numbers of fixed sensors [15]. However, several kinds of crowdsensing tasks like audio, visual, or audio-visual transmission which generates large-scale sensed data may bring high network traffic costs to participants using a 3G, 4G and 5G networks thus affecting their satisfaction. With the increased number of smartphone uptake which stands at over 4.5 billion gadgets, human mobility patterns and daily actions have increased tremendously with a possibility of many participants taking part in MCS data collection in a passive or opportunistic manner [16]. The advantages and disadvantages of MCS are summarized in Table 1.

This paper illustrates the evaluation of SiTBaM, a simulator for MCS trust. The SiTBaM is specifically designed to perform analysis and evaluation of trust in diverse environments under MCS campaigns, and support hybrid sensing paradigm. This simulation platform can visualize the obtained results of trust. The rest of the paper is organized

TABLE 1. Advantages and disadvantages of mobile crowdsensing (MCS).

Advantages	Disadvantages
• More scalable, • Low deployment cost, • Large scale, • Crowd carrier mobility, • Fine-grained measurement, • Crowd powered data collection, • Spatiotemporal coverage, • Crowd powered data analysis, • Flexibility, • Savings on computational resources, • Improved service quality, • High predictive model accuracy, • Management facilitation.	• High consumption of energy, • The optimization problem of user selection, • Takes a long time in recruitment, • Installation/maintenance cost, • Lack of scalability, • Insufficient spatial-temporal coverage.

Sources: [4][17][18][19][20][21]

as follows. A basic overview of the types of MCS schemes, and challenges, opportunities, and solutions are provided in Section 2. Details about the MCS architecture are provided in Section 3, followed by the discussion on privacy preservation and trust management of MCS in Section 4. Section 5 provides the details on MCS systems simulations and discussion. Finally, the conclusion is provided in Section 6.

II. MOBILE CROWDSENSING

Mobile crowdsensing is gaining a lot of familiarity in this era of mobile technology. According to Wikipedia, mobile crowdsensing is a mobile data-gathering technology where a large group of individuals who have mobile devices capable of sensing and computing collectively at the same time can share data and extract information to measure, map, analyze, estimate, or infer any processes of their common interest. This technique can also be summarized to mean crowdsourcing of sensor data from mobile devices which can be largely dispersed from each other. According to [12], a number of individuals, forming the crowd, is committed to performing observations of real-world phenomena of common interest through the use of mobile phones, given their capacity to sense the environment and other phenomena in the community (e.g. finding the total number of people in a restaurant, or in a cinema hall given their GPS position).

There are two common types of MCS techniques namely, participatory MCS, and opportunistic MCS [3]. In Participatory MCS paradigm, the user is actively involved and is aware of the sensing through the use of the front end applications and actively reports observations while in the case of opportunistic MCS, the user involvement is minimized and in some cases, none and often, an application can be running in the background which performs sensing and monitoring tasks with minimal or no user intervention. However another type of MCS termed as hybrid MCS can also exist, which harvests the benefits of both methods, making the number of MCS methods to be three [22]. For the task of sensing, the built-in and ubiquitous sensors of the smartphones are used either in a participatory, or opportunistic way depending on whether

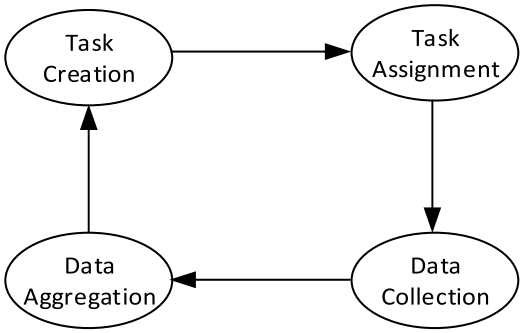

FIGURE 1. Life-cycle of MCS.

the data collection happens with or without participant involvement [7].

The mechanism of task allocation models is based on human Involvement; knowledge available to service providers (SP); and spatial distribution. In so doing the MCS tasking entities are responsible for assigning tasks to carriers, via the task assignment models. The MCS contains four stages in its life cycle namely: task creation, task assignment, data collection, and data aggregation shown in Fig. 1.

A. PARTICIPATORY TECHNIQUE

This is a type of MCS system where the participant is actively involved in the collection of data. This can include the case of photography, and filling in questionnaires. This means that the users are self-aware about sharing data with the other users in participatory sensing mode of collecting data. The participants use their own mobile devices to complete the task by collecting the data and giving the feedback regarding the results[23], and users prefer to have control over what and when to participate in a sensing campaign. This method is prone to adversarial attacks because a malicious node could easily send false information to a service provider, and it thrives from continuous input from the user [24] as the user voluntarily participates in the contribution of information. Here sensor data collection is triggered by tasks, which specify the sensing modalities like regions of interest, and sampling context based on application requests. The tasks are distributed to mobile device carriers that satisfy the tasking requirements, and people can decide to accept or refuse the task allocated. We can find that data is collected under the ''primary use'' manner in explicit sensing. Privacy in explicit sensing should guarantee that participants maintain control over the release of their sensitive information, for example, the degree of granularity and data recipients.

B. OPPORTUNISTIC TECHNIQUE

In the case of an opportunistic MCS system, the sensor data is acquired autonomously and reported to the cloud periodically without the user involvement [19]. In this method, mobile devices are involved in the process of decision making instead of the users as is the case of participatory crowdsensing [7]. In Opportunistic Sensing, users unconsciously participate

in tasks, and their devices can complete the task without human help e.g. as long as a user turns on WIFI, the task of ''sensing WIFI signal and strength'' is completed without people's intervention [15]. This scheme has less reliance on active user involvement in the process of sensing and sending information, as the data is sensed and sent automatically. This whole process takes place via the portable sensors that accompany the user participant. These portable sensors can be grouped as mobile sensors, body sensors, or vehicular sensors respectively [22]. Thus this method is majorly concerned with the passive extraction of mobile sensor data, and it aims at keeping the user involvement to the minimum [24]. In this scheme data is contributed not for a sensing task, but for users to enjoy online services like socializing on Facebook or Wechat, purchasing goods on Amazon or Alibaba, etc. in this scheme, also we get that the data is reused to enhance original services or create new services by third parties i.e., used for a second purpose.

C. HYBRID TECHNIQUE

The hybrid MCS technique is collectively the best crowdsensing system as it incorporates the benefits of the former two methods of sensing. In this, the mobile source nodes apply active sensing mode (agreeable participation in data forwarding) and passive sensing mode (via opportunistic node interaction) in the network. This is an improved crowdsensing data collection method, as it improves the accuracy of the data collected since some of the data that the user may not have been willing to divulge can easily be collected opportunistically. This method is applicable to indicate a smooth switching and collaboration between participatory and opportunistic models to overcome the disadvantages of both approaches.

III. ARCHITECTURE OF MOBILE CROW-DSENSING SYSTEM

In this section, we outline the various entities of MCS system architecture. Like mobile cloud computing, MCS is relatively a new technology with lots of potential applications but no agreed-on standard architecture exists to date [25]. This motivates this research for new and innovative architecture to suit this review that tries to emphasize on certain requirements such as privacy, cost, mobility, delay, and power consumption while trying to select the optimal compromise for the other. The architecture of the cloud-based mobile crowdsensing system consists of a cloud-based platform and a large number of smartphone users [8] is shown in Fig.2. From Fig. 2, MCS architecture contains the four major components: sensors, mobile devices, communication infrastructure, and processing infrastructure [26]. These components can further be grouped into two that is the mobile data collection components, and the web-based data server [27]. The sensors and mobile gadgets form the mobile data collection subset, and the web-based data server is composed of the communication and processing infrastructure of data.

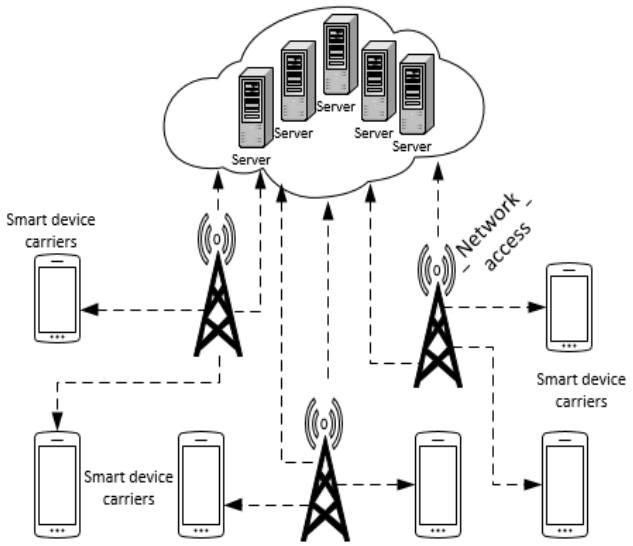

FIGURE 2. Cloud-based mobile crowdsensing architecture.

A. SENSORS

The work of sensors is data collection from the environment. It is cost-effective to use a mobile crowdsensing system technique for collecting data because it does not need specialized sensors installed everywhere, which ultimately reduces procurement, installation, and maintenance costs. The participants are equipped with the necessary hardware, software, and knowledge of the application to start gathering data as they conduct their daily life. The heterogeneous sensing capabilities pose fundamental challenges to MCS systems by affecting their two main operations truth discovery and reward distribution. The truth discovery refers to the process of aggregating and analyzing the crowd-sensed data to estimate the ground truth [28], while a reward distribution scheme is required to reward participants according to their effort levels in truth discovery process [13]. The task of sensing on the phones can be triggered manually, automatically or based on the current context.

B. MOBILE DEVICES

The task of mobile devices is to aggregate and report the collected data to the cloud server or the group owner. The subjective inputs (participants) use their mobile devices to insert data into the system about their daily locations and assessment of the phenomena. The group of mobile device users who are participating in the sensing campaign sense their surrounding environment in response to a sensing request initiated by an agent, referred to as a task publisher. Task publishers may represent machines or people and be involved in a sensing task that is time-consuming from the participant's perspective as well as consuming the device's sensing, computing, and communication resources [29].

C. COMMUNICATION INFRASTRUCTURE

The communication infrastructure is basically the data transport part tasked with the transmission of the data from the

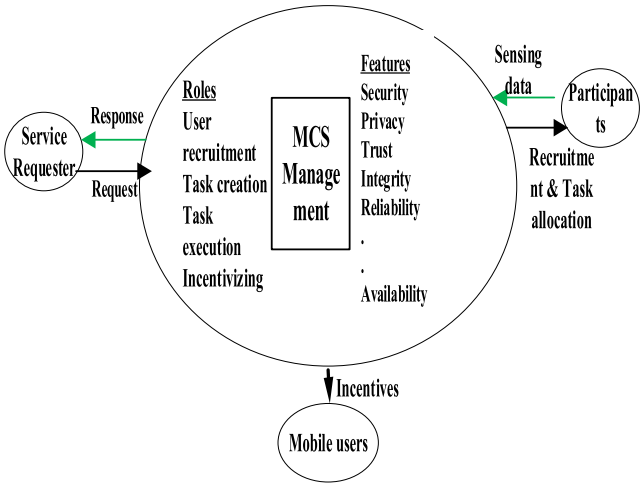

FIGURE 3. The MCS management platform.

participants to the server system. The secure crowdsensing model considers the privacy of user's data, restricts unauthorized access and enhances the quality of service in the network.

D. PROCESSING INFRASTRUCTURE

The processing infrastructure is tasked with the data storage role mostly, but also does the estimation, and inferring of the data. This layer transforms the collected low-level, single-modality sensing data into the expected intelligence through the application of the machine learning, and logic-based inference techniques [17]. The results of the processed sensed data may be displayed locally on the carriers' mobile phones or accessed by the larger public through web-portals depending on the application needs.

In MCS management there are several attributes that are taken care of together with some operations to be performed. MCS system must ensure that it guarantees security, privacy, and trust to the service requester, participants, and mobile users, when it is performing its role of user recruitment, task creation and execution, and incentivizing. Ref[30], outlines the main common incentive mechanism frameworks with their key elements as applicable in MCS which includes an auction, lottery, bargaining game, contract, market-driven, and trust and reputation. Of these incentivizing mechanisms the auction incentive is the most widely used of them all. MCS platform architecture is shown in Fig. 3.

IV. PRIVACY AND TRUST MANAGEMENT

The number of data users and participants involved in the process of data collection is growing thanks to technology. One of the key challenges posed is privacy preservation in data mining which has emerged as an absolute prerequisite for exchanging confidential information in terms of data analysis, validation, and publishing. There is an existence of ever-escalating internet phishing threats on the widespread propagation of sensitive information over the web. Equally, the dubious feelings and contentions mediated unwillingness of various information providers towards the reliability protection of data from disclosure often results in utter rejection in data sharing or incorrect information sharing. Furthermore, workers in MCS are also heterogeneous on their privacy concerns, which makes privacy preservation even more challenging. They mainly differ in (a) ratio of the private locations along their paths, (b) extend they start to treat their locations as disclosed, (c) compensation amount asked for the partial disclosure of private locations [31]. Various privacy-preserving mechanisms have been put in place to enhance the privacy preservation of the participants. According to Ref. [32], ensuring privacy-preserving in MCS system encourages mobile users to use MCS system applications and participate in sensing and data collection. Therefore, a properly designed framework for privacy preservation must support the workers to flexibly adjust on all three aspects, so as to provide most suitable participation for every worker as this is a critical principle as MCS essentially rely on these workers for data collection.

Another important issue in MCS campaigns is the trustworthiness or reliability of the data collected. Trust is a great issue as tasks are assigned anonymously and data is collected from multiple locations or participants which can be in one or another compromised leading to unreliability of the collected data [33]. It is crucial to maintain a high level of data trustworthiness which shows how much the data used are trusted, authentic and protected from abuse so that decision making should be based on precise, and certain data [34]. A user who sends altered data can get his trustworthiness degraded once detected since the MCS system computes trustworthiness, and always it runs an outlier detection algorithm to detect any form of data degradation [35]. One of the factors that can lead to data unreliability is the existence of uncertain factors like the channel or surrounding noise and the difficulty of target-sensing. At the same time, the participants can be deceived by scammers or the participants themselves can be participating in the MCS campaigns with malicious intentions thus supplying falsified data since it is sometimes difficult to identify them, especially when different task actions are not liked due to privacy protection. As participants can be participating in MCS campaign anonymously making their identities undisclosed due to privacy issues, the participants who provide falsified information cannot be identified or eliminated more so in opportunistic crowdsensing. Research has it that, if the same task is assigned to multiple participants simultaneously it can reduce the effect of malicious participation but on the hand this consumes a lot of resources. This attribute of assigning the same task to multiple users with zero rewards cannot guarantee QoS of each task to be no less than a given threshold [36]. This, therefore, poses a great challenge to create a balance between user privacy, QoS and the trustworthiness of the data or the source.

A. USER RECRUITMENT IN MCS

The malicious attackers aim to destroy the functionality of cooperative spectrum sensing so that the system cannot trust

the aggregated sensing results. This research considers four types of spectrum sensing data falsification (SSDF) attacks to test the resiliency of the proposed data aggregation scheme: ''always yes'', ''always no'', ''always false,'' and ''always random.'' Under the always yes attack scenario, the malicious secondary users (SUs) always report the presence of primary users (PUs) ignoring their real sensing results. Under the always no attack scenario, the malicious SUs always report the absence of PUs on the channel ignoring the real detection results. Under the always false attack scenario, the malicious SUs always report the opposite of their sensed outcomes. Under the always random attack scenario, the malicious SUs randomly generates a sensing result to report to the system [37]. There is no mechanism to control the behaviours of the SUs and this threatens the security of the licensed users. The major behaviours of the attackers can include but not limited to misbehaving, selfishness, cheating, and malice. An attacker can misbehave and this is the severest category of attacker behaviours as if a node misbehaves and can apply any of the other categories, decreasing the performance of spectrum sensing and sending false information to prevent other nodes from utilizing the spectrum [38]. The cooperative incentive mechanism is applied in crowdsensing participant recruitment, to try and model the cooperation between participants [39].

There arise two social dilemmas however when it comes to pricing schemes in MCS where either the requester pays rewards to participants before or after executing the task. If payment is made before task execution, participants may pay less effort in the sensing task, and if payment is made after execution of the task, the requesters may lie about the quality of sensing data in order to not to pay or to pay lee, rendering the whole exercise of participant recruitment to be futile due to false reporting schemes.

B. PRIVACY MANAGEMENT

There are various technologies that have been researched on and are in use for the application of privacy preservation in MCS systems applications. These methods sometimes require to be used to complement each other. Due to the diverse qualities of users on different tasks, task allocation is critical to all MCS systems, the efficiency of which depends mostly on the participant location information to compute the distances between tasks and workers. The longer the distance between the target user to the target location of the task, the greater the reward of completing the task, the shorter the travel distance, and the more likely that the user will accept the task and the fewer rewards the crowdsensing server will pay [40]. However, the location information may fall in the hands of an untrusted CS-server as well as the incentives, concerns about privacy leakage and security threat will discourage users from engaging in MCS. Thus, location privacy preservation should be jointly taken into account in MCS task allocation. Demands for the location privacy preservation and the task completion rate when developing an optimal task allocation method must be considered in the design of the MCS systems. There are various techniques that can be applied to ensure that the privacy preservation is maintained.

1) ENCRYPTION

Encryption is the process of decoding information thus rendering it meaningless to any unauthorized users or systems. This technique can aggregate the private data of Mobile Device Owner (MDOs) without revealing MDOs' individual data records [8]. Each participant in the sensing campaign has to obtain an encryption key to cipher his collected data and the encryption key should be known to the sensing service buyer to decipher the data. This mechanism requires a lot of computation power and resource energy which makes it sometimes unsuitable for most crowdsensing applications, particularly when it is deployed on energy-constrained mobile devices. This scheme of privacy preservation in MCS is required to secure data fusion while guaranteeing traceability, as MCS requires to balance privacy preservation against user reliability. Thus the MCS system must ensure that the data is always kept encrypted before they are transmitted to the authorized entities in the system, and remains encrypted in the system.

2) ANONYMITY

In the privacy preservation of the data and the participants in the sensing campaign, anonymity is employed in data collection and uploading of information. However, to ensure that scrupulous and malicious participants do not take advantage of this scheme, the Trust Authority (TA) can infer the true identity of a given participant, given the anonymity of the participants [18]. The pseudonym-based methods will offer anonymity to the MDOs, but they also bring significant cost and potential risk since a user may use a pseudonym for a while and drop it and switch to a new one, and increases processing time as the anonymity process gets more strict. But for better privacy, it is prudent to employ a policy of short-lived and frequently changed pseudonyms for better privacy although the privacy can again be compromised if any of the neighbors involved in the pseudonym exchange are attackers. Sometimes it is hard to achieve anonymity when both location and reputation are being incorporated into the participant's query, and if full anonymity is provided to the users, guaranteeing the trustworthiness of the reported data is impossible.

3) AUTHENTICATION

When participants are assigned tasks in a sensing campaign, sometimes it is good to use a mechanism of identifying the authenticity of the participants by ensuring that the assigned task includes information about the task description, the location of the task, the finish time of the task, and the status of the task as well as the user identities [41]. This method ensures that the participants do not submit falsified information into the system which will compromise the trustworthiness of the system, although it is seen as compromising the privacy of the users on the other hand. Therefore the MCS system is

responsible for the access control, by giving the necessary rights to authorized users [32].

4) NON-REPUDIATION

No participant should be able to change its mind (e.g. deny or modify its data) once the data has been submitted [42]. This implies that once a participant wishes to take part in a sensing campaign, they are bound by the data they submit although this is not the case for opportunistic crowdsensing data collection.

5) DATA AGGREGATION

Data aggregation is a widely used technique in wireless data networks. The data aggregation algorithms are designed to gather the data and aggregate the data to enhance the network's lifetime. This is a mechanism where participants tend to distribute their collected data among their neighbours, and Ref. [22] terms it as the process of integrating data from multiple users into one message. When a participant receives a request from the aggregation server, each participant returns his data and the remaining data of his neighbours, thus reducing the probability to successfully attribute each sensor reading to its corresponding mobile user. Performing crowd sensing with the help of many individuals leads to the collection of a large amount of data, necessitating data aggregation and processing to converted data into high- level information before being utilized by users and systems [22], which is better for decision making than when it is from a single source [17]. But an MCS service has to control the data production process since mobile devices typically support only limited filtering and aggregation mechanisms and often deliver all raw readings to the cloud [1].

6) CONFIDENTIALITY

various mechanisms should be put in place to ensure that the confidentiality of the user's information and weights in crowdsensing systems is maintained. The confidentiality of observed values or user's sensitive information collected by the cloud server (such as health data, location, address, etc.) should be protected and prevented from disclosure to other parts like to other users, the cloud server, and any attacker [43]. For example, aggregating health data, such as treatment outcomes, can lead to better evaluation of new drugs or medical devices' effects but may leak the privacy of participating patients. Thus confidentiality is the technique of ensuring that the data that is in storage or in transit is encrypted to conceal its contents and only the data owners know the plaintext.

7) VERIFICATION AND VALIDATION

verification and validation refer to the authentication and confirmation of the participant identity in the MCS network before the participants can take part in the sensing campaign. A few steps of verification, checking and anonymization through the different components can be employed to provide a higher level of privacy to the participants [42].

C. TRUST MANAGEMENT

The MCS system can be said to be trust-worthy if the user feels safe to use, and also trusts to execute tasks without secretly executing any harmful programs, and trust management is one of the factors that affect performance and lifetime of MCS [44]. The trust evaluation model calculates the trust value based on the user's communication behaviour. The presence of malicious trustees in the system is notified to the trustor in the MCS system. To enhance system trustworthiness, it is critical for the trustor to recruit users based on their personal features, e.g., mobility pattern and reputation, although it leads to the privacy leakage of participants [45]. The sensing data collected from the surrounding areas are necessarily people-centric and related to some aspects of mobile users and their social settings: where they are and where they are going; what places they are frequently visited and what they are seeing; how their health status is and which activity they prefer to do. Social event photos may expose the social relations, locations or even political affiliations of mobile users.

The spatial data collected by the carried devices might disclose mobile users' trajectories. For example, Google Maps collect the ''anonymous'' location information of drivers for real-time traffic map generation but still exposes the driving routes and trajectories of drivers. Further, the more sensing tasks the mobile users are engaged in and the richer data the users contribute to, the higher probability that their sensitive information may be exposed. Therefore, preserving the privacy of mobile users is the first-order security concern in mobile crowdsensing. If no effective privacy-preserving mechanism is on-shelf, it is of difficulty to motivate mobile users to join in mobile crowdsensing services.

There are three forms of trust in MCS: direct trust, indirect trust, and comprehensive trust. Direct trust involves issues to do with the knowledge obtained about the MCS system as direct observation. The attributes of direct trust include ability, integrity, availability, reliability, similarity, and security. On the other hand, the indirect trust involves issues revolving around the experience and the reputation gained over time about the MCS system. The indicators used to evaluate the direct trust of an MCS includes interactions, past related experiences, and relationships. The experience is constructed from the interactions between two entities, while the reputation is constructed from all the experiences towards an entity [33]. The comprehensive trust is the one that incorporates the features of all the former two types of trust.

According to Ref. [46], the size of the trust value respects the performance of the node. The malicious node always leads to declining trust value because of its bad communication behavior, while the normal node is the opposite. In this article, the sensor nodes monitor the communication behavior of their neighbors to detect whether there is any packet dropping or packet tampering. As shown in Fig. 4, node x evaluates the trust value of node y, where k_1, k_2 and k_m are the common neighbours of the node x and y.

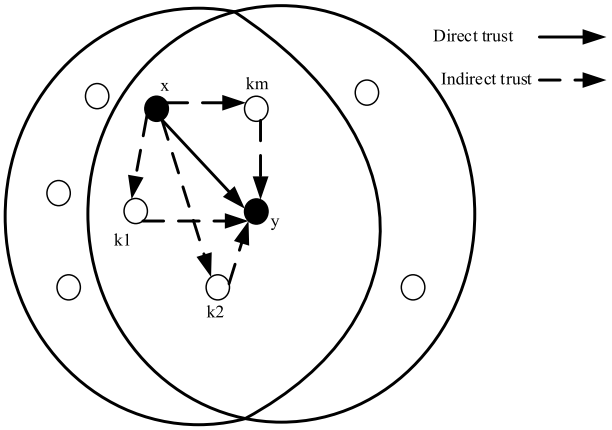

FIGURE 4. Trust components.

1) DIRECT TRUST

The research by Ganeriwal *et al.* [47], proposed a trust evaluation model that utilizes the Beta distribution to evaluate trust and proved that the trust values obey the Beta distribution tendencies. The direct trust value DT_{xy} of node x to y can be obtained by:

$$DT_{xy} = E\left(Beta\left(\alpha_{xy}, \beta_{xy}\right)\right) = \frac{\alpha_{xy} + 1}{\alpha_{xy} + \beta_{xy} + 2} \tag{1}$$

where α_{xy} denotes the number of cooperative interaction, and β_{xy} denotes the number of non-cooperative interactions among the nodes x and y.

The original Beta-based trust evaluation model does not consider the impact of external factors on the communication interaction among the nodes, such as the packet loss caused by network congestion. This problem can be solved by the introduction of an abnormal attenuation factor q to improve the original model. The abnormal attenuation factor q is the probability of malicious attacks which is represented below:

$$q = \frac{Num_{intrusion}}{Num_{detection}} \tag{2}$$

where $Num_{intrusion}$ is the number of node non-cooperative interaction caused by malicious attacks, and $Num_{detection}$ is the total number of node non-cooperative interactions. The attenuation of the number of non-cooperative nodes detected by node x to y can reduce the influence of external factors on the trust value. The accuracy of trust evaluation is improved compared with the original model and the formula becomes:

$$DT_{xy} = E\left(Beta\left(\alpha_{xy}, \beta_{xy}\right)\right) = \frac{\alpha_{xy} + 1}{\alpha_{xy} + q\beta_{xy} + 2} \tag{3}$$

2) INDIRECT TRUST

To improve the value trust accuracy it is necessary to obtain the indirect trust of the node y from the common and adjacent nodes between nodes x and y. The expression for an indirect trust of neighbor node k to node y is:

$$IT^{k}_{xy} = DT_{kx}.DT_{ky} \tag{4}$$

To filter all false evaluations from malicious nodes, all indirect trusts collected from adjacent nodes need to be disposed to exclude the false evaluations which are above the deviation threshold Th_{dev}. The deviation degree of indirect trust D_k is:

$$D_k = \frac{1}{m-1} \sum_{u-1, u \neq k}^{m} \sqrt{\left(IT^{u}_{xy} - IT^{k}_{xy}\right)^2} \tag{5}$$

If the degree of deviation of indirect trust is greater the Th_{dev}, the indirect trust is dropped so that the false evaluation of malicious node can be dealt with.

3) COMPREHENSIVE TRUST

In the process of evaluating trust, apart from considering the direct trust, the indirect trust a combination of these two forms of trust can be performed so that comprehensive trust value of node x to node y can be obtained as shown below:

$$T_{xy} = \mu.DT_{xy} + \frac{(1-\mu)}{m} \sum_{k=1}^{m} IT^{k}_{xy} \tag{6}$$

where μ is the weight of direct trust and in this research, $\mu = 0.5$. Therefore the direct, indirect, and comprehensive trust in MCS can be employed depending on the scenario to be evaluated that can guarantee the best results.

D. CHALLENGES OF PRIVACY AND TRUST MANAGEMENT IN MCS

There are many challenges when it comes to MCS technology. One of the major challenges is how to balance anonymity in safeguarding user privacy while maintaining the reliability of the data and/the source. This is because mobile crowdsensing has become a popular paradigm to collaboratively collect sensing data from pervasive mobile devices, and since the devices used for mobile crowdsensing are owned and controlled by individuals with unpredictable reliability, varied capabilities, and unknown intentions, data collected with mobile crowdsensing may be untrustworthy [9].

Credibility improvement of the data supplied by the MCS system is another challenge. This is because MCS systems are subject to collusion attacks where a group of malicious users can collaboratively send fake information to mislead the system [29]. Defending the data credibility requires strong defense mechanisms to curtail the collusion of participants. Ref. [39] proposed a two-phase group-buying based auction mechanism for recruiting workers in MCS, which makes it hard for participants to know each other and maybe even supply wrong sensing information.

The concept of employing users and devices to collect data from the real world poses significant social and technological and economic challenges, solutions, and opportunities. From the social point of view, if users of the MCS systems are not motivated, they can provide unreliable data which will not be meaningful. Various methods of motivation can be applied like incentivizing participants, and also ensuring their privacy. Some technological challenges which can emerge include issues like compatibility of hardware.

TABLE 2. Challenges, solutions, and opportunities of privacy and trust management in mobile crowdsensing.

Challenges	Solutions	Opportunities	Source
- Incentivizing human user, - Quality of sensed data, - Reliability of sensed data, - Participant selection, - Trust level discrimination, - Security and privacy, - Big data processing, - Heterogeneous vendors of sensors, - Incompatible design and types of sensors, - Requirements of coverage quality, - Participant recruitment, - Hybrid networking, - Satisfying the requirements of incentive mechanism, - Varied user grouping, - Cross community sensing and mining, - Requirements of data timeliness, - Energy consumption of mobile sensing devices.	- Green MCS solution that is energy aware, - Middleware solution for MCS applications, - Use of recommender systems, - Big data and cloud platform, - Application of privacy multi-scheme, - Incentive management, - Anonymization, - Location privacy protection, - Maximize task assignment clearance rate, - A two-stage privacy-preserving mechanism, - Multi-task selection.	- Prediction, - Real-time data delivery, - Efficient data collection, - Enables visualization, - Spatial sampling diversity, - Influence maximization, - Improved anywhere anytime user engagement, - Bridge of the gap between space and physical space, - Cross-space data mining.	[48][4] [11][14] [16][17] [18][20] [49][26] [50][51] [29] [52]

TABLE 3. Simulation setup for SiTBaM.

Parameter	Value
Number of user ranges	100-10000
Duration of time slot	60 sec
Task duration	1800 sec
Number of task ranges	100-1600
Damage level range	0-50
% of malicious users	0-100
Quality of data values	0-1
Interactions	500
Cooperative threshold	0.6
Uncooperative threshold	0.3

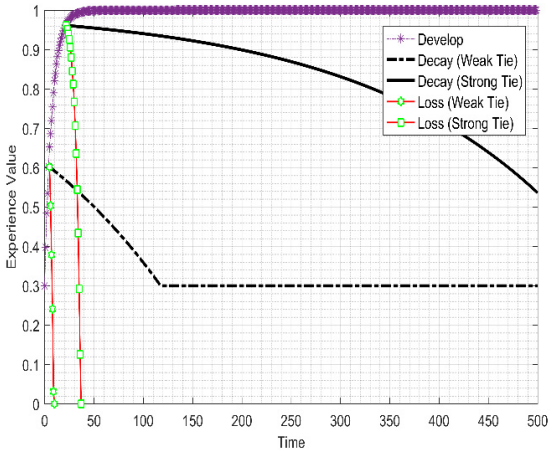

FIGURE 5. Experience model with development, decay, and loss trends.

TABLE 2 presents a summary of the various MCS challenges, solutions, and opportunities. As depicted in the table there are a number of challenges since MCS technology in a new and emerging area still that requires to be researched.

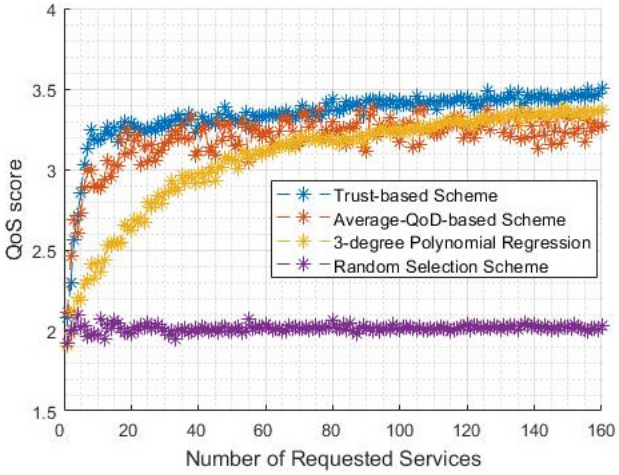

FIGURE 6. Quality of services (QoS) vs, number of requested services.

V. SIMULATION RESULTS AND DISCUSSIONS

In this research, the new approach was proposed for SiTBaM used for evaluating trust in MCS paradigm. The SiTBaM simulation setup parameters are as shown in table 3. From the table, the quality of data values was set at 0 to 1, which implies that 0 is least QoD, while 1 is highest QoD. The number of tasks was varied from 100 to 1600 in multiples of 400, and their corresponding damage level versus the percentage of malicious users recorded as demonstrated in the simulation results.

The assumptions of the proposed model in relation to trust evaluation are:

1. The higher the number of tasks the lower the damage level
2. The higher the number of malicious users the higher the damage level.
3. The higher the number of quality users the higher the probability density.

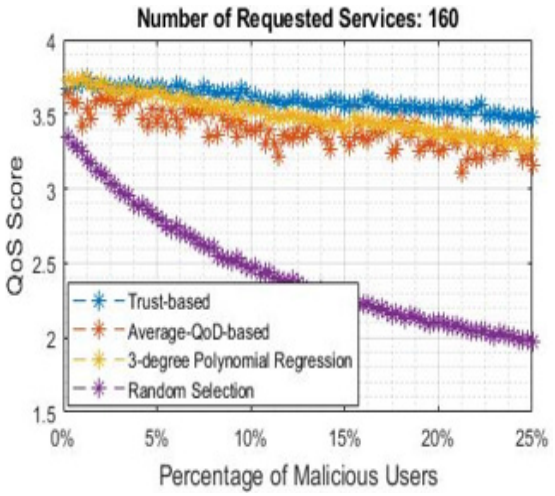

FIGURE 7. Percentages of Malicious users vs. QoS Score.

The Experience Model is normalized in the range [0,1] and it specifies three trends: Development, Loss, and Decay. The development trend implies that the cooperative interaction experience is in the increase, the loss trend indicates that the cooperative interaction experience is decreasing, while the decay trend indicates that the experience in the cooperative interaction is either increasing or decreasing as there exists neutral or no interaction that is taking place. The decay trend is the worst as it is unpredictable in regard to the future trend. In the experience model, the experience between any two users can be established and updated by the use of an aggregation model on any virtual interactions. The reputation of each user can be calculated based on all the experiences between all users, and a value of trust relationship is also calculated by aggregating the experience and the reputation. Therefore to find the trustworthiness of the system users, the user experience and reputation are very critical. Due to cooperative interactions the experience increases and uncooperative interactions cause the experience to decrease. Consequently if not interactions occur at all, the experience decays. Therefore the determining factors for the decrease, increase, or decay of experience include the intensity of interactions, interaction scores, and current experience value of the MCS system, as shown in Fig. 5.

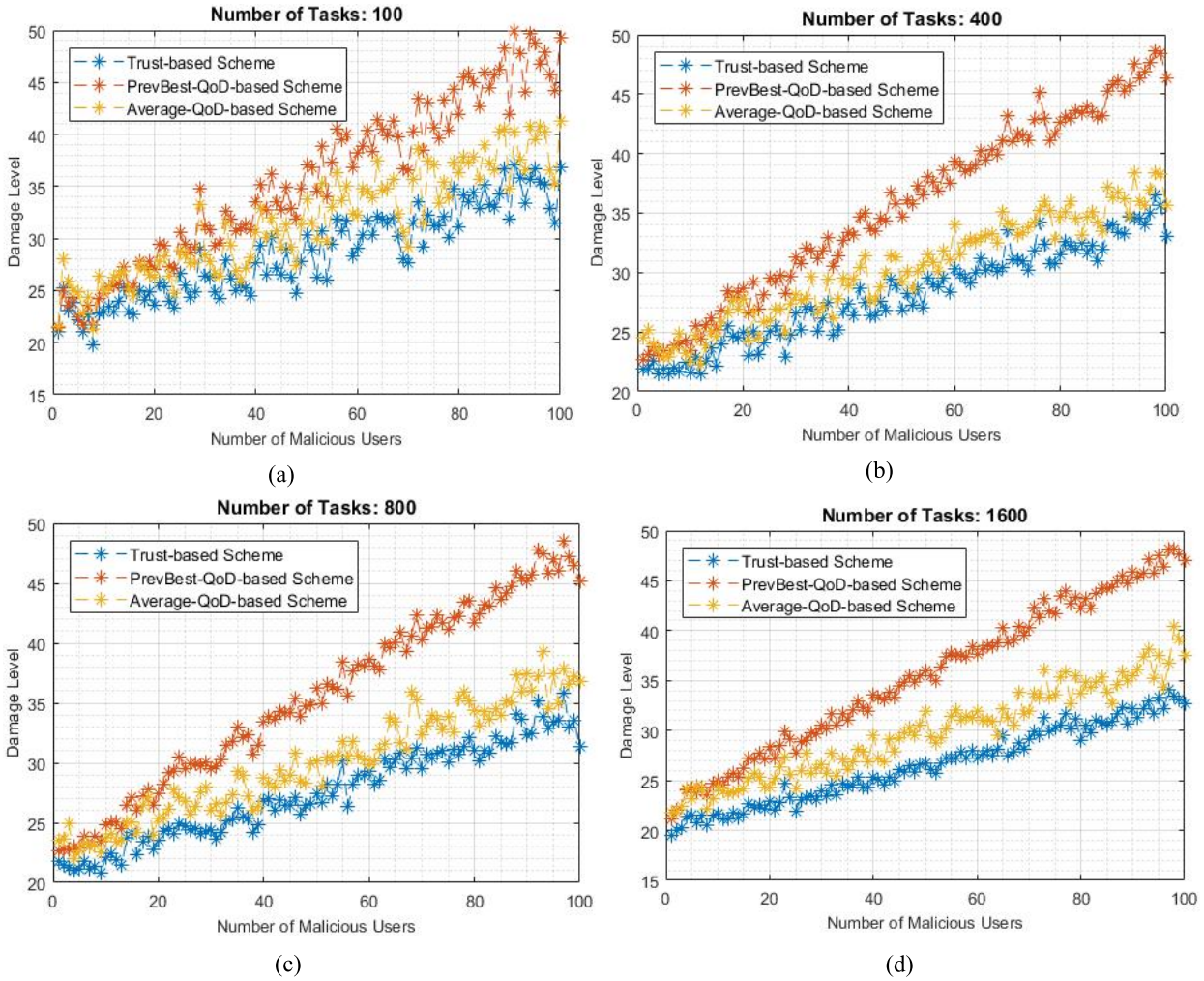

FIGURE 8. (a)-(d) Comparison of Damage levels in Trust-based, vs. PrevBest-QoD-based, vs. Average-QoD-based Schemes.

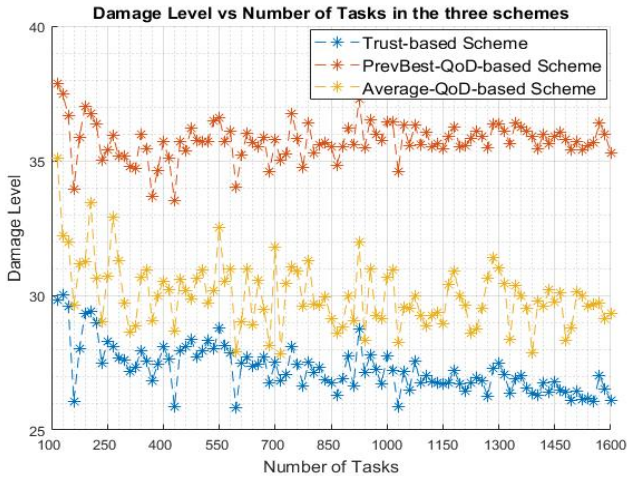

FIGURE 9. Comparison of Schemes with varying task numbers.

From Fig. 6, a series of interactions was randomly created where the number of interactions (n) was set at n = 500, and cooperative threshold and the uncooperative threshold was set at 0.6, and 0.3 respectively. The experience model was generated as shown with the development, decay, and loss trends.

From Fig. 6, the QoS improves significantly when the number of requested services increases for trust-based schemes, average-QoD-based schemes, and 3-degree polynomial regression schemes. However, the QoS remains the same when the random selection scheme is employed. All this however from the figure indicates and confirms that the QoS is higher when the Trust-based scheme is employed.

From Fig. 7, when the percentage of malicious users increases the quality of service (QoS) decreases in that order. This means that the presence of malicious users affects the performance of MCS system QoS, and the measure has to be put in place to ensure that this existence of malicious users is reduced to minimal margin to yield better results.

From Fig. 8 (a)-(d) the damage levels of data values versus the varying the number of malicious users were compared in three different schemes Trust-based scheme, Average-QoD-based scheme, and the PrevBest-QoD-based Schemes. It was observed that the trust-based scheme provides the least damage level to the obtained data even after the number of malicious users is increased. Actually as the number of malicious users is increased the damage level decreases but on a marginal value. The PrevBest-QoD-based schemes record the highest damage level even as the number of malicious users increases.

From Fig. 9, the damage level is high when the number of tasks is lower based on all the three schemes of trust. Therefore when the number of the tasks is higher the better the results in terms of the damage caused. And from this, there is a big marginal gap between the damage levels when the PrevBest-QoD-based scheme is used compared to the rest of the schemes.

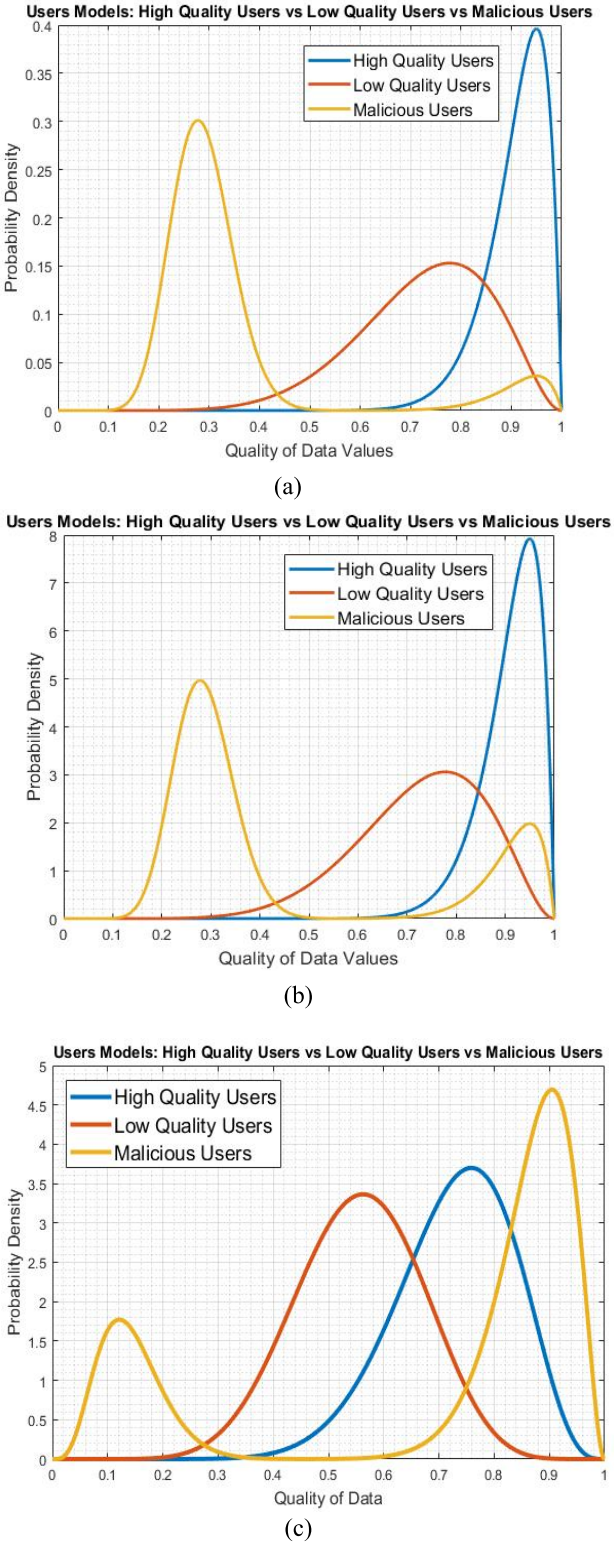

FIGURE 10. (a)-(c) The User Models of different MCS systems.

From Fig. 10 (a) the QoD range is between the intervals (0,1) and the highest quality users produced the highest quality-of-data (QoD) scores in most sensing tasks with the highest distribution QoD value is 0.95, with a probability

density function (PDF) value of 0.4. The low-quality users produced the lowest and below-average QoD scores by recording the highest score of 0.78 with the PDF value of at 0.15. The malicious users produced the above-average QoD scores of 0.28 and PDF of 0.3.

From Fig. 10 (b) the QoD interval ranges are (0 to 1) and the highest quality user-produced QoD value of 0.95, at a PDF value of 8. The low-quality user produced the highest QoD value of 0.78 with PDF value of 3. The malicious user accounted for highest QoD value of 0.28, with PDF of 5. This malicious user recorded higher value than the low-quality user.

In Fig. 10 (c) the QoD interval remain (0 to 1) and the highest quality user records the highest QoD value of 0.76 with the PDF of 3.7. The low-quality user records an above-average QoD of 0.56 and a PDF of 3.4. However again the malicious user records highest QoD values than both the high-quality user and the low-quality user of 0.9, and PDF of 4.7. These cases in Fig. 10 (a) to (c) demonstrate that the QoD can vary from system to system and the PDF values recorded vary for different users (highest quality, lowest quality, and malicious users). This depicts that the system trust levels are equally different across the various models.

VI. CONCLUSION

The evolution of mobile devices has led to the vast evolution of mobile crowdsensing technology, where mobile devices are used to sense, collect, and transmit information seamlessly. In this survey, we discussed the overview of MCS, schemes of MCS, and the challenges, opportunities, and solutions of MCS. Since the MCS is applicable in almost all of life scenarios, the applications of MCS in terms of its importance was discussed. The MCS architecture was discussed where the MCS framework and the architecture are highlighted in broad. Since a large number of participants take part in sensing campaigns, their privacy is of utmost importance and hence the MCS systems privacy-preservation and trust management were discussed. This is very crucial because even if there are incentives, mobile device users can shy off from participating in sensing campaigns if their privacy is not guaranteed. The simulations were based on Trust-based scheme, and it was compared with other schemes. The results obtained indicate that trust-based scheme offers the best results when compared to its counterparts which were discussed as follows.

1. The damage level is lower under the trust-based scheme even in the event of an increase in the number of tasks or number of malicious users.
2. The QoS value is high even when the presence of malicious users tends to increase in number.
3. The QoD scores produced depends on the security level of the MCS system. The QoD score can be high for high-quality users, or malicious user, but always the QoD score is average for the case of low-quality users.

In summary, the performance of trust-based mechanisms in privacy and trust management in MCS systems is high, and more algorithms should be developed to enhance the level of trust in the MCS application.

CONFLICT OF INTEREST

The authors declare no conflict of interest for the publication of this article.

REFERENCES

[1] M. Marjanovic, A. Antonic, and I. P. Zarko, "Edge computing architecture for mobile crowdsensing," *IEEE Access*, vol. 6, pp. 10662–10674, 2018.

[2] J. Feng, T. Li, Y. Zhai, S. Lv, and F. Zhao, "Ensuring honest data collection against collusive CSDF attack with binary-minmaxs clustering analysis in mobile crowd sensing," *IEEE Access*, vol. 7, pp. 124491–124501, 2019.

[3] C. Fiandrino, A. Capponi, G. Cacciatore, D. Kliazovich, U. Sorger, P. Bouvry, B. Kantarci, F. Granelli, and S. Giordano, "CrowdSenSim: A simulation platform for mobile crowdsensing in realistic urban environments," *IEEE Access*, vol. 5, pp. 3490–3503, 2017.

[4] F. Wang, L. Hu, R. Sun, J. Hu, and K. Zhao, "SRMCS: A semantic-aware recommendation framework for mobile crowd sensing," *Inf. Sci.*, vols. 433–434, pp. 333–345, Apr. 2018.

[5] S. Yang, J. Bian, L. Wang, H. Zhu, Y. Fu, and H. Xiong, "EdgeSense: Edge-mediated spatial-temporal crowdsensing," *IEEE Access*, vol. 7, pp. 95122–95131, 2019.

[6] C. Jiang, L. Gao, L. Duan, and J. Huang, "Scalable mobile crowdsensing via peer-to-peer data sharing," *IEEE Trans. Mobile Comput.*, vol. 17, no. 4, pp. 898–912, Apr. 2018.

[7] M. Pouryazdan, C. Fiandrino, B. Kantarci, T. Soyata, D. Kliazovich, and P. Bouvry, "Intelligent gaming for mobile crowd-sensing participants to acquire trustworthy big data in the Internet of Things," *IEEE Access*, vol. 5, pp. 22209–22223, 2017.

[8] J. Lin, D. Yang, M. Li, J. Xu, and G. Xue, "Frameworks for privacy-preserving mobile crowdsensing incentive mechanisms," *IEEE Trans. Mobile Comput.*, vol. 17, no. 8, pp. 1851–1864, Aug. 2018.

[9] 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, Jun. 2017.

[10] M. Arafeh, M. El Barachi, A. Mourad, and F. Belqasmi, "A blockchain-based architecture for the detection of fake sensing in mobile crowdsensing," in *Proc. 4th Int. Conf. Smart Sustain. Technol. (SpliTech)*, 2019, pp. 1–6.

[11] M. Li, Y. Gao, M. Wang, C. Guo, and X. Tan, "Multi-objective optimization for multi-task allocation in mobile crowd sensing," *Procedia Comput. Sci.*, vol. 155, pp. 360–368, Jan. 2019.

[12] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, and P. Bouvry, "A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2419–2465, Apr. 2019.

[13] H. Cai, Y. Zhu, Z. Feng, H. Zhu, J. Yu, and J. Cao, "Truthful incentive mechanisms for mobile crowdsensing with dynamic smartphones," *Comput. Netw.*, vol. 141, pp. 1–16, Aug. 2018.

[14] C. M. Angelopoulos, O. Evangelatos, and S. Nikoletseas, "A user-enabled testbed architecture with mobile crowdsensing support for smart, green buildings," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 573–578.

[15] Z. Peng, X. Gui, J. An, T. Wu, and R. Gui, "Multi-task oriented data diffusion and transmission paradigm in crowdsensing based on city public traffic," *Comput. Netw.*, vol. 156, pp. 41–51, Jun. 2019.

[16] S. Bradai, S. Khemakhem, and M. Jmaiel, "Real-time and energy aware opportunistic mobile crowdsensing framework based on people's connectivity habits," *Comput. Netw.*, vol. 142, pp. 179–193, Sep. 2018.

[17] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "From participatory sensing to mobile crowd sensing," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PERCOM WORKSHOPS)*, Mar. 2014, pp. 593–598.

[18] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fog-based crowdsensing on the Internet of vehicles," *J. Netw. Comput. Appl.*, vol. 134, pp. 89–99, May 2019.

[19] E. Wang, Y. Yang, and K. Lou, "User selection utilizing data properties in mobile crowdsensing," *Inf. Sci.*, vol. 490, pp. 210–226, Jul. 2019.
[20] H. Li, D. Liao, G. Sun, M. Zhang, D. Xu, and Z. Han, "Two-stage privacy-preserving mechanism for a crowdsensing-based VSN," *IEEE Access*, vol. 6, pp. 40682–40695, 2018.
[21] J. Xu, W. Bao, H. Gu, L. Xu, and G. Jiang, "Improving both quantity and quality: Incentive mechanism for social mobile crowdsensing architecture," *IEEE Access*, vol. 6, pp. 44992–45003, 2018.
[22] H. Vahdat-Nejad, E. Asani, Z. Mahmoodian, and M. H. Mohseni, "Context-aware computing for mobile crowdsensing: A survey," *Futur. Gener. Comput. Syst.*, vol. 99, pp. 321–332, Oct. 2019.
[23] M. Marjanović, L. Skorin-Kapov, K. Pripužic, A. Antonic, and I. P. Žarko, "Energy-aware and quality-driven sensor management for green mobile crowd sensing," *J. Netw. Comput. Appl.*, vol. 59, pp. 95–108, Jan. 2016.
[24] M. Mehdi, G. Mühlmeier, K. Agrawal, R. Pryss, M. Reichert, and F. J. Hauck, "Referenceable mobile crowdsensing architecture: A healthcare use case," *Procedia Comput. Sci.*, vol. 134, pp. 445–451, Jan. 2018.
[25] J. B. Abdo and J. Demerjian, "Evaluation of mobile cloud architectures," *Pervas. Mobile Comput.*, vol. 39, pp. 284–303, Aug. 2017.
[26] A. Suliman, H. Otrok, R. Mizouni, S. Singh, and A. Ouali, "A greedy-proof incentive-compatible mechanism for group recruitment in mobile crowdsensing," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 1158–1167, Dec. 2019.
[27] X. Li and D. W. Goldberg, "Toward a mobile crowdsensing system for road surface assessment," *Comput. Environ. Urban Syst.*, vol. 69, pp. 51–62, May 2018.
[28] F. Shi, Z. Qin, D. Wu, and J. A. Mccann, "Effective truth discovery and fair reward distribution for mobile crowdsensing," *Pervas. Mobile Comput.*, vol. 51, pp. 88–103, Dec. 2018.
[29] R. Azzam, R. Mizouni, H. Otrok, A. Ouali, and S. Singh, "GRS: A group-based recruitment system for mobile crowd sensing," *J. Netw. Comput. Appl.*, vol. 72, pp. 38–50, Sep. 2016.
[30] T. Luo, S. S. Kanhere, J. Huang, S. K. Das, and F. Wu, "Sustainable incentives for mobile crowdsensing: Auctions, lotteries, and trust and reputation systems," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 68–74, Mar. 2017.
[31] G. Luo, K. Yan, X. Zheng, L. Tian, and Z. Cai, "Preserving adjustable path privacy for task acquisition in mobile crowdsensing systems," *Inf. Sci.*, to be published, doi: 10.1016/j.ins.2018.12.013.
[32] N. P. Owoh and M. M. Singh, "Security analysis of mobile crowd sensing applications," *Appl. Comput. Inform.*, to be published, doi: 10.1016/j.aci.2018.10.002.
[33] N. B. Truong, G. M. Lee, T.-W. Um, and M. Mackay, "Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2705–2719, Oct. 2019.
[34] M. Yu, H. Lin, and J. Hu, "A data trustworthiness enhanced reputation mechanism for mobile crowd sensing," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, vol. 2, Jun. 2018, pp. 743–747.
[35] B. Kantarci and H. T. Mouftah, "Mobility-aware trustworthy crowdsourcing in cloud-centric Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2014, pp. 1–6.
[36] T. Hu, M. Xiao, C. Hu, G. Gao, and B. Wang, "A QoS-sensitive task assignment algorithm for mobile crowdsensing," *Pervas. Mobile Comput.*, vol. 41, pp. 333–342, Oct. 2017.
[37] J. Wang, I.-R. Chen, J. J. Tsai, and D.-C. Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," *Comput. Commun.*, vol. 116, pp. 90–100, Jan. 2018.
[38] M. Khasawneh and A. Agarwal, "A collaborative approach towards securing spectrum sensing in cognitive radio networks," *Procedia Comput. Sci.*, vol. 94, pp. 302–309, Jan. 2016.
[39] T. Liu, Y. Zhu, and L. Huang, "TGBA: A two-phase group buying based auction mechanism for recruiting workers in mobile crowd sensing," *Comput. Netw.*, vol. 149, pp. 56–75, Feb. 2019.
[40] H. Shen, G. Bai, Y. Hu, and T. Wang, "P2TA: Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing," *J. Syst. Archit.*, vol. 97, pp. 130–141, Aug. 2019.
[41] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.
[42] T. Dimitriou and I. Krontiris, "Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications," *J. Netw. Comput. Appl.*, vol. 100, pp. 24–34, Dec. 2017.
[43] G. Xu, H. Li, C. Tan, D. Liu, Y. Dai, and K. Yang, "Achieving efficient and privacy-preserving truth discovery in crowd sensing systems," *Comput. Secur.*, vol. 69, pp. 114–126, Aug. 2017.
[44] K. Z. Ghafoor, L. Kong, A. S. Sadiq, Z. Doukha, and F. M. Shareef, "Trust-aware routing protocol for mobile crowdsensing environments," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 82–87.
[45] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, "Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, to be published.
[46] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Comput. Sci.*, vol. 131, pp. 1156–1163, Jan. 2018.
[47] S. Ganeriwal, M. B. Srivastava, and L. K. Balzano, "Reputation-based framework for high integrity sensor networks," *J. ACM Trans. Sens. Netw.*, vol. 4, no. 3, pp. 132–146, 2008.
[48] K. Yi, R. Du, L. Liu, Q. Chen, and K. Gao, "Fast participant recruitment algorithm for large-scale vehicle-based mobile crowd sensing," *Pervas. Mobile Comput.*, vol. 38, pp. 188–199, Jul. 2017.
[49] M. Abououf, R. Mizouni, S. Singh, H. Otrok, and A. Ouali, "Multi-worker multi-task selection framework in mobile crowdsourcing," *J. Netw. Comput. Appl.*, vol. 130, pp. 52–62, Jan. 2019.
[50] K. Agrawal, M. Mehdi, M. Reichert, F. Hauck, W. Schlee, T. Probst, and R. Pryss, "Towards incentive management mechanisms in the context of crowdsensing technologies based on TrackYourTinnitus insights," *Procedia Comput. Sci.*, vol. 134, pp. 145–152, Jan. 2018.
[51] M. E. Gendy, A. Al-Kabbany, and E. F. Badran, "Maximizing clearance rate of reputation-aware auctions in mobile crowdsensing," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 5–6.
[52] F. Wang, W. Jiang, G. Wang, and S. Guo, "Influence maximization by leveraging the crowdsensing data in information diffusion network," *J. Netw. Comput. Appl.*, vol. 136, pp. 11–21, Jun. 2019.

DOROTHY MWONGELI KALUI received the M.Sc. degree in information systems from the University of Nairobi, Kenya. She is currently pursuing the Ph.D. degree with the University of Science and Technology Beijing, China. She is also a Lecturer with the Department of Computer Science, School of Computing and Informatics, Meru University, Kenya. Her current research interests include spatial databases, mobile data privacy, the IoT security, and application of information technology in organizations especially in financial institutions.

DEZHENG ZHANG is currently the Director of the Beijing Key Laboratory of Knowledge Engineering for Materials Science, University of Science and Technology Beijing, China. He is also the Director/Professional Lead for knowledge engineering in specific domains, especially in traditional Chinese medicine and materials science. He is also Promoting, developing, and supporting research and teaching programs with the University of Science and Technology Beijing. His main research directions cover data mining and knowledge discovery, ontology-based knowledge base construction, and intelligent information processing.

GEOFFREY MUCHIRI MUKETHA received the B.Sc. degree in information science from Moi University, in 1995, the M.Sc. degree in computer science from Periyar University, in 2004, and the Ph.D. degree in software engineering from Universiti Putra Malaysia, in 2011. He has wide experience in teaching and supervision of master's degree students. He is currently an Associate Professor and the Dean of the School of Computing and Technology, Muranga University of Technology. His research areas include software and business process metrics, software quality control, Component-based software engineering, data privacy, and technology adoption.

JARED OKOYO ONSOMU received the B.S. and M.S. degrees in computer science from the University of Nairobi, Kenya, in 2009 and 2014, respectively. His research interests are in the areas of artificial intelligence and machine learning.