Emerging Sensing and Secure Computing in Mobile Crowdsensing System

Sasireka V
Shyamala Ramachandran

DeepScience

Emerging Sensing and Secure Computing in Mobile Crowdsensing System

Sasireka V

Department of Computer Science and Engineering, M.S. Engineering College, Bengaluru, India-600025

Shyamala Ramachandran

Department of Information Technology, University College of Engineering- Tindivanam, India- 600025

DeepScience

Published, marketed, and distributed by:

Deep Science Publishing, 2025
USA | UK | India | Turkey
Reg. No. MH-33-0523625
www.deepscienceresearch.com
editor@deepscienceresearch.com
WhatsApp: +91 7977171947

ISBN: 978-93-7185-545-7

E-ISBN: 978-93-7185-433-7

https://doi.org/10.70593/978-93-7185-433-7

Citation: Sasireka, V., & Ramachandran, S. (2025). *Emerging Sensing and Secure Computing in Mobile Crowdsensing System*. Deep Science Publishing. https://doi.org/10.70593/978-93-7185-433-7

Preface

Mobile Crowdsensing Systems (MCS) rely on the collaborative participation of a multitude of individuals equipped with mobile devices capable of sensing and computing. Together, they share data and extract information to observe, map, analyze, estimate, or predict various processes of common interest. This approach offers the advantage of low deployment cost and extensive geographical coverage, making it applicable in various domains such as transportation, environmental monitoring, smart cities, pervasive healthcare, and more. However, MCS systems often encounter challenges related to security, privacy, and trust. The presence of motion sensors like accelerometers and gyroscopes in smartphones is crucial for monitoring our real-world surroundings. Unfortunately, these sensors also make us vulnerable to privacy invasion attacks, where leaked private information can reveal details about human behaviors, physical characteristics, and location. Furthermore, MCS systems are susceptible to side-channel attacks, where the operation of basic sensors can inadvertently leak sensitive data in mobile crowdsensing applications. While traditional cryptography methods can address some security and privacy concerns, they are not feasible for resource-constrained smart mobile or Internet of Things devices, limiting their application in MCS. In light of these issues, this chapter proposes an innovative Proactive Defense Mechanism using Blockchain based Mobile Crowdsensing (BMCS) that aims to intercept, disrupt, or deter attacks or threats before they can occur, ensuring the security of the mobile crowd sensing process. The proposed approach has been thoroughly analyzed, and the security proofs demonstrate that it significantly enhances the level of security in MCS.

Keywords: Mobile crowdsensing, security, proactive defence mechanism, cyber-attacks, Blockchain based Mobile Crowdsensing, Blockchain.

Sasireka V.

Shyamala Ramachandran

Table of Contents

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

DeepScience
Open Access Books

Introduction

The advancement of portable gadgets propels a novel sensing paradigm known as mobile crowdsensing. Equipped with an array of elegant sensors and intelligent devices, the portable gadget possesses the capability to collect diverse sets of information for specific purposes. In a formal sense, mobile crowdsensing pertains to a collective of mobile users collaborating to undertake extensive sensing tasks across urban environments by utilizing their portable devices. Figure 1 illustrates a typical workflow of mobile crowdsensing. As depicted in Figure 1, three distinct types of participants emerge: the requester (Task worker), the crowdsensing platform, and the task performer.

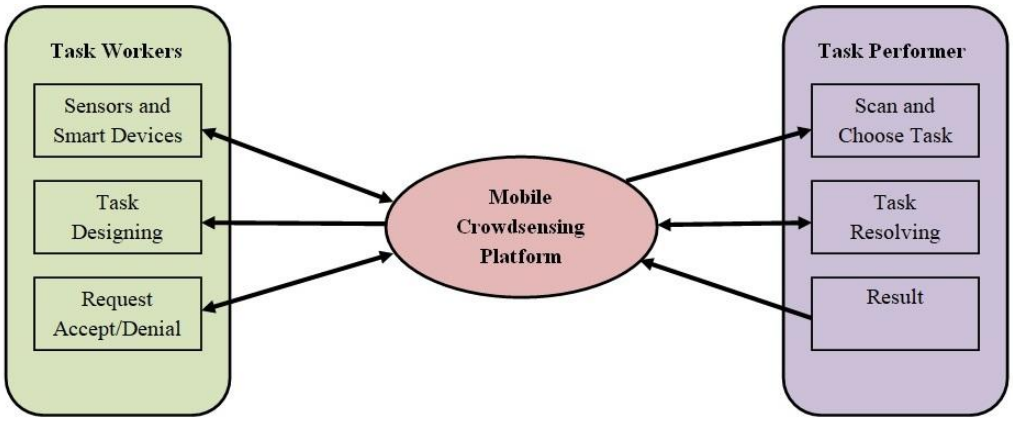

Figure 1: Mobile Crowdsensing- Workflow

The mobile crowdsensing process encompasses eight stages: task design, task release, task scanning, task selection, task resolution, result submission, acceptance/refusal, and integration. When a requester desires to initiate a task, they must present their task requirements to the crowdsensing platform. The task performers within the crowdsensing platform scan the available tasks and opt for those that are suitable.

Following task completion, the performers submit their results to the platform, where the requester assesses their quality. If deemed satisfactory, all the results are consolidated, and the task concludes. Due to the convenience of deployment and communication, mobile crowdsensing has been widely implemented in numerous scenarios, including smart transportation, environmental monitoring, and data labeling. While mobile crowdsensing presents an unprecedented solution for data collection and processing, it also introduces a host of new challenges. One of the primary concerns lies in privacy preservation when designing a mobile crowdsensing scheme. Previous studies predominantly focus on safeguarding the privacy of task performers, particularly during the result submission stage. However, certain tasks may also pose privacy risks during the task release stage due to the platform's lack of complete trustworthiness. The platform may deduce requesters' privacy based on their tasks. Furthermore, task access control poses another issue that requires attention. In mobile crowdsensing, tasks are stored on the platform, accessible to anyone in the system. This open access may result in subpar task results, if unqualified performers accept the tasks. Moreover, task access control effectively safeguards task information from being obtained by irrelevant entities, such as the crowdsensing platform. Therefore, task access control and a proactive defense mechanism are crucial for mobile crowdsensing.

Proactive defensive mechanisms are methods and strategies used in crowdsensing to avoid or lessen possible security and privacy problems related to collecting data from a large number of people or devices in a crowd. In order to learn more about a community or area's inhabitants, crowdsensing entails gathering data from sensors, smart phones, or other linked devices that they may be carrying. Crowdsensing proactive defense mechanisms include Secure Communication Protocols, Access Control and Authentication, Behavioral Analysis and Anomaly Detection, Risk Assessment and Threat Modeling, Privacy-Preserving Data Collection, Participant Awareness and Consent, and Secure Data Storage and Processing. This manuscript proposed a proactive defense mechanism in crowdsensing by incorporating the access control and authentication mechanisms, so that the data shall be preserved against the various attacks. The contribution of the proposed work is as follows.

The proposed system provides an enhanced level of security to the mobile crowdsensing by performing accessing control and authentication validation mechanisms.

Maintaining the privacy of task performers and requesters is one of the key goals of the suggested system. To the best of our knowledge, very little of the material currently in publication addresses requesters' privacy. The crowdsensing platform is not entirely reliable, though. The crowdsensing platform may infer information about requesters and endanger their privacy if jobs are submitted to it without any safeguards. The proposed Blockchain based Mobile Crowdsensing (BMCS) is suitable for multi-

environment, resource and types of users and provides a better access control mechanism than the existing methods.

The organization of the manuscript is preceded with the literature review in section 2 to identify the drawbacks of the existing methodologies and to frame the objectives of the proposed work. The section 3 describes the proposed work of providing access control and the method is analyzed in the section 4. The manuscript is concluded in the section

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

DeepScience
Open Access Books

Literature Review

Privacy preservation is the major challenge of the mobile crowdsensing technique and various researchers actively proposed novel methodologies in preserving the privacy. Some of the notable research activities that act as the motivation for this proposed work is summarized in this section. B.Zhao et al. (2023) devised a secure aggregation algorithm (SecAgg) [11] that employs the threshold Paillier cryptosystem to combine training models in an encrypted format. The authors introduced a unique hybrid incentive mechanism that merges the reverse Vickrey auction and the posted pricing mechanism, which has been proven to be honest yet unsuccessful. Theoretical analysis and experimental evaluation in a practical MCS scenario (human activity recognition) demonstrate the effectiveness of CrowdFL in safeguarding the privacy of participants while maintaining operational efficiency.

J.Zhang et al. (2023) addressed the privacy-preserving task assignment for heterogeneous users (PTAH) problem [12] in mobile crowdsensing. In this study, users are divided into two groups: private users with location privacy requirements and public users without such requirements. The authors developed a privacy-preserving mechanism to obfuscate the actual location of private users. Furthermore, they constructed a relationship graph based on the locations of users and tasks. J.Wang et al. (2023) introduced a personalized location privacy incentive in the form of a double MCS auction mechanism [13]. This innovative approach allows workers to determine the extent of location information they disclose to the platform, providing personalized location privacy protection. Additionally, workers are given the flexibility to submit multiple bids for tasks of interest and perform a subset of tasks if they emerge as winners. The auction mechanism enables the platform to select winning requesters and workers, thereby achieving optimal sensing service accuracy.

Y.Jiang et al. (2023) proposed a learning-based mechanism [14] that comprises two components: 1) privacy-preserving task release and allocation, and 2) accurate and efficient task allocation. In the first part, the authors devised a location-based symmetric key generator that enables two parties to generate a symmetric key independently,

eliminating the need for fully trusted authorities. By leveraging this key generator and Proxy Re-encryption, a privacy-preserving protocol was developed to safeguard location information during task release and allocation. In the second part, a reinforcement learning-based task allocation algorithm was designed to optimize the selection of winners, ensuring high accuracy and efficiency. Y.Cheng et al. (2023) designed a lightweight privacy-preserving sensing task matching algorithm [15] that upholds location privacy, identity privacy, sensing data privacy, and reputation value privacy, while minimizing computation and communication overhead for sensing vehicles. To prevent reputation values from being tampered with and to select reliable sensing vehicles, the authors devised a privacy-preserving reputation value equality verification algorithm and a privacy-preserving reputation value range proof algorithm. Additionally, a three-factor reputation value update algorithm was constructed to efficiently and accurately update the reputation values of sensing vehicles.

R.Ganjavi et al. (2023) introduced an efficient edge-assisted MCS scheme [16] that protects the privacy and anonymity of participants. This scheme effectively tackles the join-and-leave problem, demonstrating minimal computational cost and communication overhead that remains constant. B.Zhu et al. (2023) introduced an innovative approach to data aggregation, leveraging the Chinese remainder theorem [17] for privacy preservation. By incorporating blinding factor and Paillier homomorphic encryption technology, the system not only ensures the privacy of the collected data, but also enhances its robustness. The authors further enhanced the privacy aspect by introducing a secure multicast communication technology based on the Chinese remainder theorem, which allows only designated sensing nodes to access the task. Additionally, an efficient signature scheme was devised to ensure data integrity.

S.Sangeetha et al. (2023) proposed a cutting-edge technique for preserving location privacy in a crowdsensing environment, utilizing blockchain technology [18]. This novel approach overcomes the limitations of traditional crowdsensing methods and safeguards the location information of workers through a privacy preserving algorithm. P.Chaudhari (2023) presented an innovative scheme for privacy-preserving and cost-effective work distribution, incorporating a fine-grained access control system [19]. The scheme employs a ciphertext-policy attribute-based encryption method with a hidden access policy, ensuring the privacy of both data requesters and data collectors. Y.Cheng et al. (2023) introduced a groundbreaking framework [20], named PRTD, which combines privacy preservation and reputation-based truth discovery. This framework accurately generates ground truths for sensing tasks while maintaining data privacy. The authors achieve this by utilizing the Paillier algorithm and Pedersen commitment to protect sensing data privacy, weight privacy, and reputation value privacy. Furthermore, they devised a privacy-preserving reputation verification algorithm, based on reputation

commitment and zero-knowledge proof, to detect tampered reputation values and select trustworthy mobile users based on a concept of reliability level.

Based on the literature study performed in this section, related to the security of the mobile crowdsensing technology, the following challenges have been witnessed and act as the motivation factor for the objective framing of this proposed work.

The existing works relies on centralized storage, in which the level of trust is not to the acceptable level.

The quality of the data collected through the mobile devices are prune to the location and hence questions the guarantee of the location secrecy.

The objectives of the proposed work are as follows.

To provide location based security to the data stored in centralized storage or distributed storage.

To employ blockchain technology for maintaining a registry of data and to preserve the privacy of the data gathered through the mobile crowdsensing.

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

Proposed Work

Preliminaries

The preliminaries used in this proposed work of blockchain based proactive defense mechanism in the mobile crowdsensing are as follows.

- Bilinearity property: The close groups ‘a’ and ‘b’ are cyclic with prime p, q to the generator G such that e: G*G=G_T and is defined as if, $\forall a, b \in G$ and $x, y \in Z$, then, $e(a,b)^{xy} = e(a^x, b^y) = 1$
- Non-degeneracy property: e(G,G)≠1.

Proposed blockchain based Proactive Defense Model

The proposed system is composed of the blockchain technology which involves the contribution of entities namely, the task requester, task verifiers, workers and the blockchain registers for data storage and validation purposes. The task requesting node acts as the requester or a worker depending on the condition. As depicted in Figure 2, the node desiring to publish a task transforms into a task requester and disseminates the task information through the blockchain. The nodes yearning to undertake the task upload their operational data and present a deposit to establish a contract with the task requester. Following the completion of the preregistration process, the smart contract will be automatically triggered to select competent workers from the preregistering worker set for the specific task. The deposit will either be returned to the workers who were unsuccessful in preregistering or were not selected. Upon accomplishing the task, the workers upload the result metadata, while the tangible data is encrypted and stored in the distributed database, patiently awaiting the task requester's evaluation. Ultimately, the evaluation result will be submitted, and if deemed qualified, the workers shall receive their well-deserved reward.

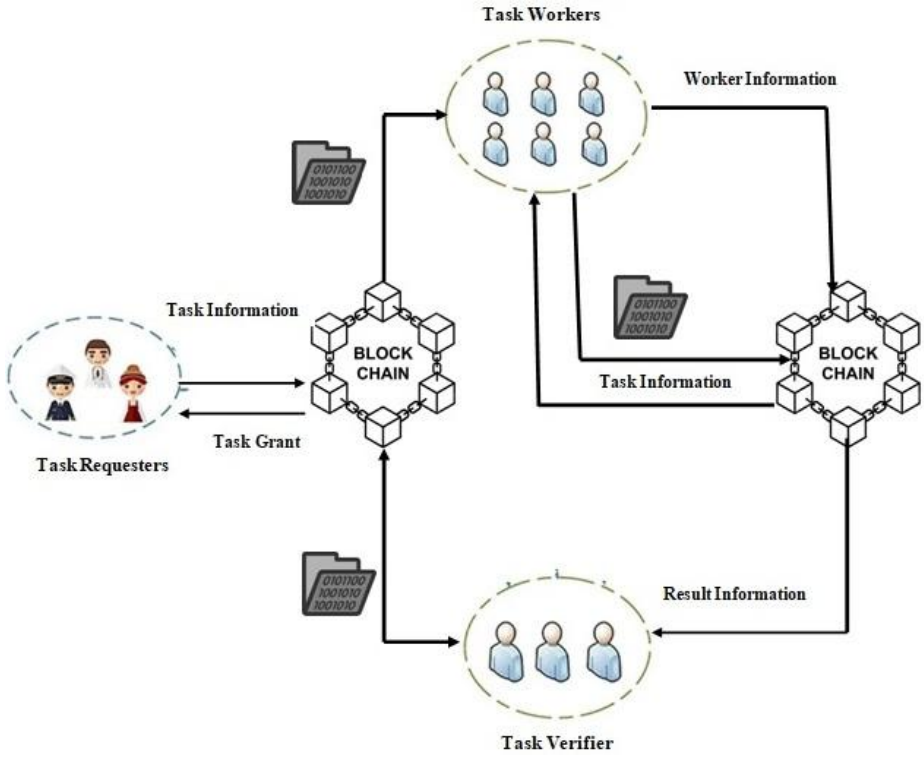

Figure 2: Proposed Blockchain based Mobile Crowdsensing

As illustrated in Figure 2, the innovative model introduced a decentralized system called Blockchain based Mobile Crowdsensing system (BMCS), portraying three central characters: a task seeker, laborers, and an examiner, all able to engage in a collaborative network. To enhance comprehension of the process of selecting workers, we have provided a list of symbols and their corresponding explanations in Table 1.

Table 1: Parameter Nomenclature

Notations	Parameter Description
T_r	Task Requester
T_w	Task Worker
T_v	Task Verifier
T_s	Sub Target
N_w	Number of workers
N_{Ts}	Number of sub targets
L_w	Worker's location
A_w	Area of the worker

A task requester, known as Tr, has the ability to create its own identity and account on the blockchain in a secretive manner. Through this account, Tr can post tasks and conduct transactions. The account holds various properties related to the requester,

including tokens and reputation. Tr can utilize the blockchain to publish tasks and select suitable workers.

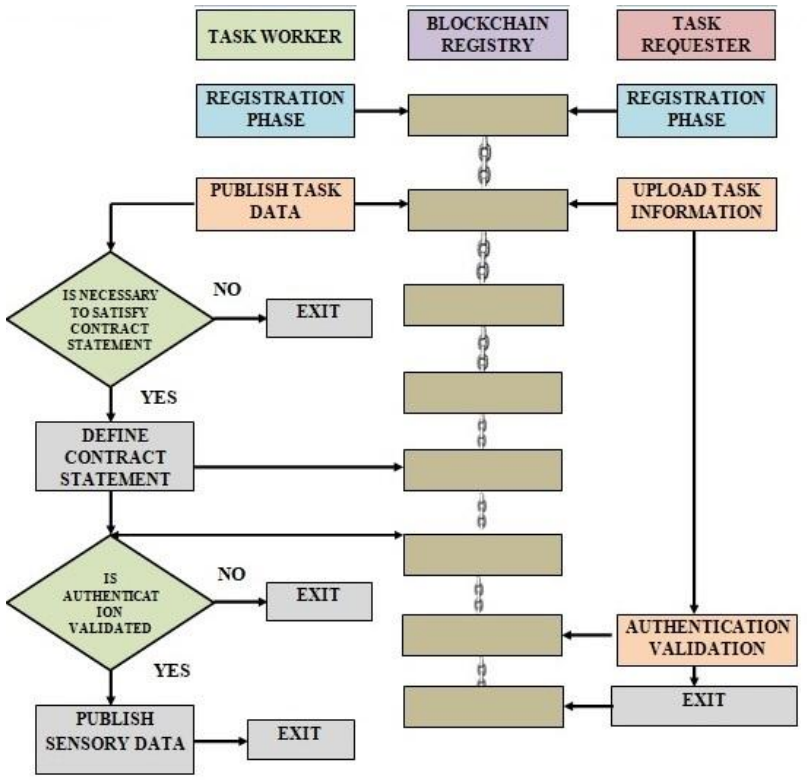

Figure 3: Proposed Work- Flow process

Similarly, a worker, referred to as Tw, is a user created anonymously on the blockchain. The worker's account contains their reputation and an acceptable travel budget, Tb, for completing tasks. Prior to receiving tasks, Tw must submit relevant working information to the blockchain and set aside a deposit for worker selection. The flow process of the proposed work is depicted in Figure 3. A verifier, known as Tv, plays a role in the verification and consensus process. Tv is a miner node selected through the proof of work and is responsible for managing transaction information on the blockchain. In order to protect the true location, a cloaked area is generated for a worker, Tw. This cloaked area is defined as (ai, fi), where ai represents a spatial anonymous area based on the worker's true location within our proposed algorithm, and fi represents the probability density function. To ensure maximum task coverage, the area required for the task is divided into multiple sub-areas. If the worker's working area is circular, the division interval is a multiple of the radius of the worker's working coverage area. Similarly, the entire target area is divided into multiple subtargets. This allows for the achievement of full coverage of the target area by focusing on the full coverage of the subtargets within the subareas.

To provide a more comprehensive explanation of the crowdsensing communication process, we have devised seven distinct stages within the BMCS framework as demonstrated in Figure 3. In the Initial Setup Phase, BMCS generates sets of public and private keys for the mobile users who participate in the crowdsensing activities. The users are responsible for safeguarding their private keys, which will be utilized during the signature process. During the Task Release Phase, the task requester R disseminates the specific task details along with its signature and public key to the blockchain. This ensures the authenticity and efficacy of the task. Simultaneously, the crowdsensing contract, containing the task information and the requirements for worker execution, is posted by the task requester as a transaction on the public blockchain. Any worker who fulfills the contract conditions can then sign the contract. To ensure fairness in trade, the requester creates a smart contract outlined in Algorithm 1. This contract encompasses information about the requester, the workers, and the task itself. It operates autonomously on the public blockchain according to a predefined protocol.

In the Preregistration Phase, upon receiving the broadcasted task information, workers who wish to undertake the task may initiate a transaction. This transaction includes their work-related information as well as a certain deposit required to sign the contract. The deposit serves as a preventive measure against fraudulent activities and will be refunded if the worker fails during preregistration. Successful preregistration grants the worker participation in the final selection process. Due to the setting of P and Q, the final set of selected workers will be a subset of the preregistered worker set. Once the Preregistration Phase concludes, the smart contract responsible for the final worker selection is automatically triggered. If a worker is chosen as the final worker, their corresponding deposit will be returned. To ensure data quality and protect location privacy, the Worker Selection Methodology for Crowdsensing (WSMC) is employed to select suitable workers from the preregistered worker set. Moving on to the Upload Result Phase, after completing the sensing task, the worker must utilize a digital signature and public key to upload the sensory results and await evaluation from the task requester. Considering the limitation of storage space on the blockchain, only the metadata is uploaded, while the actual data is stored in a distributed database. Furthermore, due to the transparent nature of the blockchain, it is imperative to encrypt the result information using the task requester's public key to prevent plagiarism.

During the Quality Evaluation Phase, once the task requester receives the result information, they proceed to evaluate its quality using a specific evaluation method. In our article, the task requester quantifies and normalizes the sensing data, subsequently dividing it into two sets: qualified and unqualified. These sets reflect the satisfaction levels of the results in relation to the task's requirements (Reqt). Finally, in payment phase. If the uploaded data is deemed qualified, the smart contract automatically initiates payment to the workers, in addition to returning their deposit. The number of workers

chosen to work in a particular area ai will be successful in signing the work contract and the increase in success rate of worker selection process is defined in equation 1.

$$\forall i = T_w \sum_{j=0} x_j \leq T_j; \sum_{j=0} x_j s_j \geq Q_j \quad ..(1)$$

Where, Tw is the task workers, Tj is the threshold rate of process and the Qj is the total number of process in the crowdsensing. After the worker acquires the task information, the smart contract will be triggered. As each worker possesses self-awareness of their whereabouts, they can utilize their precise location to refine the outcomes achieved in the initial stage and deliberate whether or not to embrace the assigned tasks. In the event of refusal, in order to minimize the excessive workload, the system model will solely reevaluate workers within the specific subarea that the user declined. The second step's optimization objective is depicted by equation 2.

$$S = \{\{T_{w1}, T_{w2}, T_{w3} \dots \dots T_{wn}\} \oplus \{T_{s1}, T_{s2}, T_{s3} \dots \dots T_{sn}\}\} \quad (2)$$

The key generation by the entities for the creation of block and to access the data from the BMCS incorporates the public key cryptography, involving public key and the private key for encryption and decryption processes. The algorithm for the pre-registration process is illustrated in Table 2.

Table 2: Pre-Registration Process

Algorithm 1: Pre-Registration process
Input: T_{Wr}- Task work region; x_{ixj}- Task work matrix; T_a- Task coverage area; T_g- Task coverage goal; N_w- Number of Workers; T_{wt}- Worker threshold region.
Output: R_w- Contracted result of worker
Processes:
1: Initialize the parameters
2: If $\sum_{i \in N} x_i s_i < T_{wt}$; then
3: If $N_w < T_{wt}$; then
4: $N_w + += 1$
5: $x_{i \times j} \leftarrow 1$
6: Then, Initiate new register in blockchain
7: Return Registration Success
8: Else
9: Return Registration Failed
10: End if
11: End if
12: Return completed
13: End process

The Table 2 defines the pre-registration process of the BMCS and initiates the blockchain registration process. The algorithm 2 is based on the two vital parameters

namely the Tg- Task coverage goal; Twt- Worker threshold region. In the next phase, we implement a two-step process to carry out the selection of workers. This process involves the utilization of BMCSs and BMCSf. BMCSs refers to the initial screening of workers, while BMCSf denotes the subsequent refinement of selection results by the workers themselves. During the initial step of worker selection, our proposed approach introduces two effective techniques to address the uncertainty issue arising from location anonymity in the first stage. The latter approach is employed in this article. To tackle the optimization objectives for WSMCs, we then combine the efficient greedy algorithms that have been put forth based on the partial set cover problem.

In our proposed model, the selection process replaces the exact location of the user with a cloaked area. This enables the workers to receive tasks. Additionally, a distance-based travel cost model is utilized, where the Euclidean distance serves as the measuring unit for the sensing cost between workers and subtargets. Moreover, we extensively examine the querying algorithms for uncertain spatiotemporal data. This involves the utilization of existing range query, nearest neighbors, top-k, and other methods to propose querying techniques. Within the cloaked area, denoted as $z \in a$, there exists a substantial number of evenly distributed location points. We calculate the geometric centroid of all these points to determine the expected location of the worker. This calculation is then used to establish the expected distance matrix, represented by equation 3.

$$d_{i,j} = D\left(\int_{i=j=Ta}^{N} z f_i(z) dz\right) \tag{3}$$

The initial step involves the calculation of the likelihood that worker i can access subarea j, represented as $p_{i,j}$. To reduce the cloaked area a_i, a simple pruning technique is employed, resulting in the coincident area a_i, which is the intersection between a_i and a circular area centered at target j with a radius of r_i. By combining this with f_i, the probability that a_i contains worker i can be determined, which is equivalent to the probability $p_{i,j}$ that worker i's travel scope includes target j, as defined in equation 4.

$$p_{i,j} = \left(\int_{i=j=Tw}^{N} z f_i(z) dz\right) \tag{4}$$

Subsequently, using the probability $p_{i,j}$, the expected distance $d_{i,j}$ between the intersection area a_i and the target can be calculated, as defined in equation 5.

$$d_{i,j} = \frac{D\left(\int_{i=j=Ta}^{N} z f_i(z) dz\right)}{p_{i,j}} \tag{5}$$

The proposed model adopts a worker selection strategy that combines the greedy approach in the initial stage. Although this strategy may not be optimal, as it makes the best choice at each step, it can be refined through iterations of the algorithm. This allows for the selection of the most suitable worker for a subarea, resulting in cost-effective worker-target pairs and real-time updates to the coverage of subarea targets. The iteration process continues until the coverage goal is

achieved or the worker's travel budget is depleted. The cost effectiveness of a worker wi, where i ∈ N, and a target tj, where j ∈ M, is calculated according to equation 6.

$$\varphi_{ij}^{N} = \frac{d_{i,j}}{\max\left(1-x_i,\frac{1}{x_j}\right)+\epsilon} \tag{6}$$

In equation 6, di,j represents the expected distance, while the denominator represents the expected coverage contributed by worker wi. The matrix vector u denotes the currently covered portions of the subarea targets. If a subarea target is fully covered, its corresponding value in u will be set to 1, with a value range of [0,1]. The algorithm for worker selection is illustrated in Table 3. The worker selection is the vital algorithm, which determines the authentication of the incoming workers.

Table 3: Algorithm- Worker Registration Phase

Algorithm 2: Worker Authentication Phase

Input: T_w- Total Mobile workers; T_{st}- Task sub target; B_v- Budget vector; I_T- Threshold for iteration

Output: x_{i*j}- Worker selection matrix

Processes:

1: Initialize the parameters
2: While ($T_u < T_w$ and $B_v < T_{st}$) do
3: If ($T_u == T_u*$), then
4: If($B_v == B_v*$), then
5: $x_{i,j} \leftarrow 1$
6: $T_U \leftarrow \max\left(1 - x_i, \frac{1}{x_j}\right)$
7: If (U_{ij}==1), then
8: $T_U \leftarrow {T_U}/{T_j}$
9: End if
10: $B_v \leftarrow B_{v-1} - d_{ij}$
11: If I_T=0; then
12: $W \leftarrow W/w_{ij}$
13: End if
14: End if
15: End while

The method for estimating distance is proposed based on anticipated probabilities, and Algorithm 2 is introduced for the purpose of selecting the most cost-effective pair of worker–target (i, j) with probabilities pi,j. To achieve the desired convergence, an upper-bound threshold R is set, serving as a convergence parameter, which allows the algorithm to be stopped in the expected probabilistic approach. This threshold is specifically designed for experimental purposes and enhanced efficiency. The first step involves updating the coverage proportion in u, which is known as the expected coverage vector and is later sent to the workers in the second step. Unlike traditional crowdsensing systems where there is a risk of user-sensitive information being leaked during the registration phase, BMCS utilizes pseudonymous Bitcoin-like addresses to represent

task requesters and workers. This innovative approach allows for privacy preservation without the need for revealing the true identity of individuals involved in completing a crowdsensing task. Additionally, we have developed a location-privacy-preserving approach based on spatial cloaked areas, which replaces the true location of a worker with a corresponding cloaked region when accepting task information. This prevents the true locations of workers from being exposed to the public. As a result, BMCS provides dual protection for identity privacy and location privacy. Assuming the number of workers is represented by n, the number of subtargets by m, and the number of continuous sampling points in each cloaked area by s, the time complexity of our proposed uncertain distance estimation method is O(nms). For the expected probabilistic method, the time complexity is O(nmR) due to the limitation imposed by the number of iterations R. Given the uncertainty of anonymous locations, it is possible that the selected worker may not have access to the subtargets. Therefore, the assignment results need to be fine-tuned in the second step using the workers' exact locations, while ensuring that the overall coverage is not affected. However, if each worker simply selects the closest target to save cost, it may result in the selected workers exceeding the need of the subarea, which can lead to overcoverage. To address this issue, we have proposed additional constraints to limit the overall changes resulting from fine-tuning in the second stage. The algorithm for fine tuning the task workers is illustrated in Table 4.

Table 4: Alrogithm- Task Workers Fine Tuning

Algorithm 3: Task workers fine tuning process

Input: W_i – Present worker; T_{st} – Sub target; T_b- Budget for travel; v- Target covered vector; I_t – Iteration threshold.

Output: Y_w- Worker selection matrix

Processes:

1: Initializing the parameters
2: For all T_{st} in W_i do
3: $x_{i,j} \leftarrow x_{ij}^{*} - \frac{x_{i,j}}{K_{i,j}}$
4: End for
5: While $T_b(LT) < T_b(ST)$, do
6: If $T_{st} < T_w$, then
7: If choosing i<j<v
8: $x_{i,j} \leftarrow 1$
9: $T_b(LT) \leftarrow max\left(1 - \frac{x_{i,j}}{K_{i,j}}\right) + LT$
10: If $T_b(LT) == T_b(LT)^{*}$; then
11: Return, Authenticated Task worker
12: Else, abort process
13: End if
14: End if
15: End processes

Algorithm 4 presents the refined algorithm for the selection of workers during the second step. In a similar manner, it continuously chooses the appropriate worker wi for the subtarget, employing a certain probability to prevent excessive coverage. Unlike Algorithm 3, the proposed approach aims to fulfill the initial constraint, thus any

modifications to the selection in xi,j will incur a penalty. Consequently, the cost-effective score for each choice can be determined using equation 7.

$$\varphi_{i,j}^{2} = \frac{\frac{x_{i,j}}{T_b} + 1 - x_{ij}^{*}}{\min(1 - \frac{x_{i,j}}{T_b}) + \epsilon} \quad (7)$$

This score represents the ratio between the cost of the second step and the expected coverage provided by worker wi for the subtarget tj ∈ t, which is calculated using the same method as in the first step. The probabilities used to select workers for the task in the second step differ from those in the first step as well. Equation 8 is used to calculate pi,j for a given subtarget j.

$$p_{i,j} = 1 - \frac{\varphi_{i,j}^{2}}{\max(\varphi_{i,j}^{2})} \quad (8)$$

The objective with this probability is to prevent excessive coverage of the overall target while simultaneously reducing the likelihood of expensive tasks. Without it, workers would be chosen repeatedly for the subtargets until their travel budgets are depleted.

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

Results and Discussion

This section describes the performance analysis and the discussion on the performance of the proposed Blockchain based Mobile CrowdSensing (BMCS) model. The section is initiated with the illustration of experimental settings for the proposed work and is preceded with the analysis of the work in terms of security, computational cost, task cost. To scrutinize the performance of the quality control model BMCS in this article, a devised experimental environment based on Ethereum is employed. The software environment is Python 3.5. The hardware environment comprises a 2.60 GHz Core(TM) i7 CPU, 20 GB, and Win10 system of 64bits. The simulation strictly adheres to the protocols and patterns that may be utilized in the real-life scenario of crowdsensing. The dataset utilized was introduced and the execution of performance analysis of the proposed work follows suit. The parameter settings for the proposed work are delineated in Table 5 along with the specification of default settings. For the sake of simplicity, the model is experimented with circular areas

Table 5: Parameter definition for the proposed work

Parameters	Range of Specification	Default Settings
Total workers (T_w)	100-1000	200
Total Sub-targets (T_{st})	100-500	200
Transfer limit (T_b)	50-200m	100m
Cloaking Model	Rectangular, Hexagon, circular	Circular
Cloaking radius (C_r)	10.5-40% of mapping area	25.5%
Task Goal (T_g)	50-100%	90%

For every worker, the cloaked region is randomly selected within the circular map, covering between 12.5% and 37.5% of the total area. Each subtarget aims for complete (100%) task coverage, though this target is not fully met because of the cloaked positions. The coverage goal (g) varies from 50% to 90%, with 90% set as the default. The parameters R and R* both range between 20 and 50. Every experiment is repeated 100 times, and the average performance across these trials is reported as the final result. In the actual sensing process, the proposed model first takes into consideration the

running time of block generation. The ability of the model to swiftly generate blocks is deemed more crucial than the efficiency of task completion. The running time of generating a block encompasses the period of Merkle tree generation in the consensus and the production of a new block. The running time of the method that measures the proposed worker selection time is also taken into account for data analysis. Subsequently, the success rate and the time cost of the initial preregistration stage are contemplated, which can be influenced by the proposed data control parameters P and Q. Additionally, the task coverage (TU) and task cost (TC) are introduced. In many instances, due to the constraints of the number of workers and budget, the expected coverage g may not be accomplished assuming given worker locations. Thus, the proposed work comprehensively considers the task coverage and cost and suggests a novel evaluation indicator PI (penalized indicator), which is normalized within the range of [0,1] using the min–max method. A lower PI value implies higher coverage and lower cost, indicating a superior outcome.

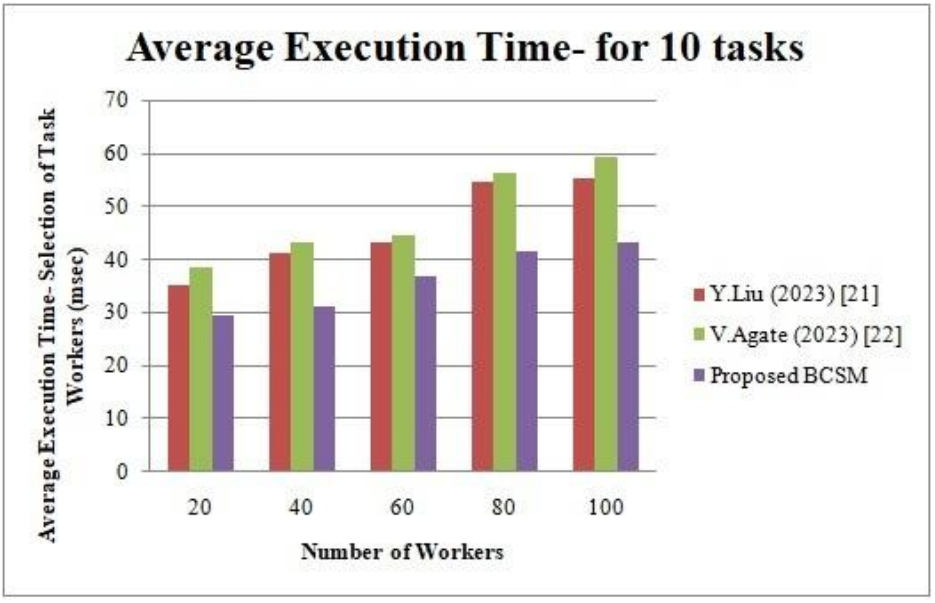

Figure 4(a): Average Execution time for 10 tasks

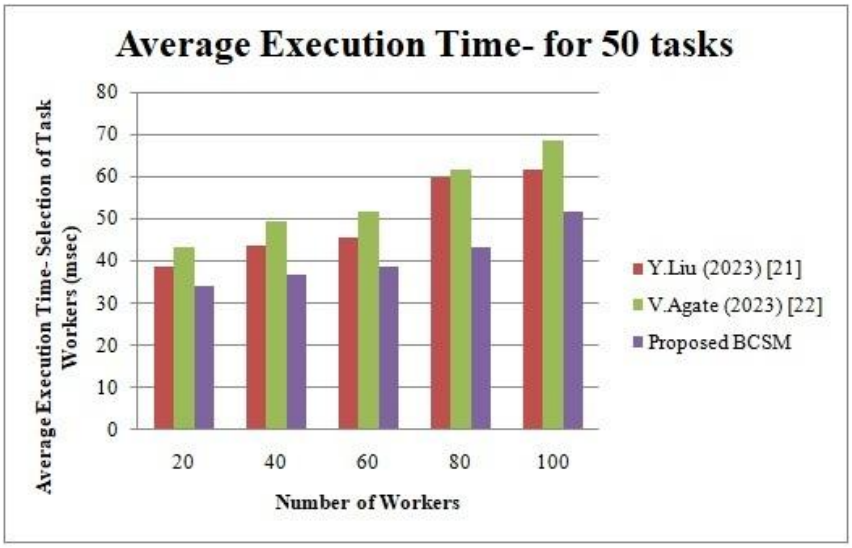

Figure 4(b): Average Execution time for 50 tasks

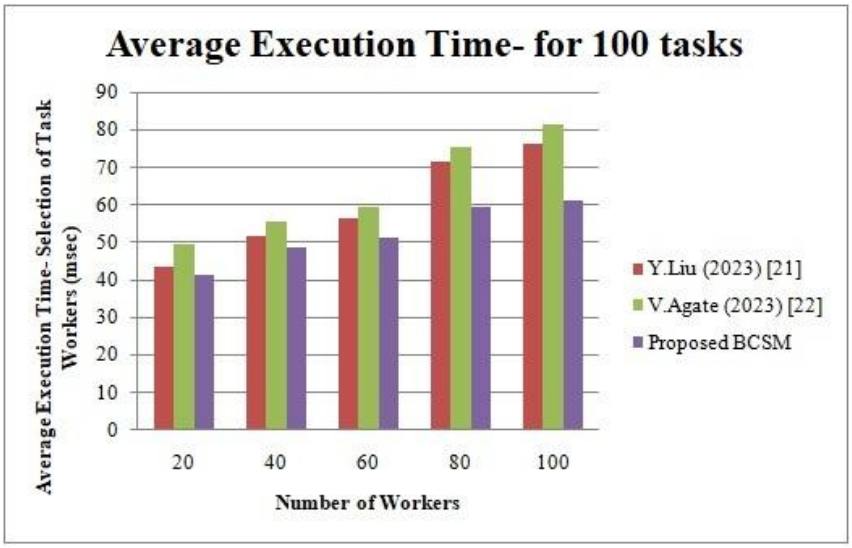

Figure 4 (c): Average Execution time for 100 tasks

As illustrated in Figure 4(a), the average block generation time increases as the number of workers grows, though it consistently remains within the millisecond range. The execution time for block generation is primarily influenced by the worker count involved in the task. This occurs because a larger number of workers results in a larger Merkle tree structure within the block. In order to analyze the performance of the two-stage worker selection approach WSMC proposed in this article, the other worker selection approaches like TaskMe (Y.Liu [21]) and ActiveCrowd (V.Agate [22]) were compared. Due to different experimental environments, we have retained its core ideas and adapted

it to fit our model. Fifty tasks were published to analyze average statistics. As shown in Fig. 4(b), and 4(c) among the three methods, the running time of ActiveCrowd is the longest, and the running time of TaskMe is slightly shorter than ActiveCrowd. The time of our proposed scheme is the shortest, and the magnitude of increase with the number of workers is not as sharp as the other two schemes.

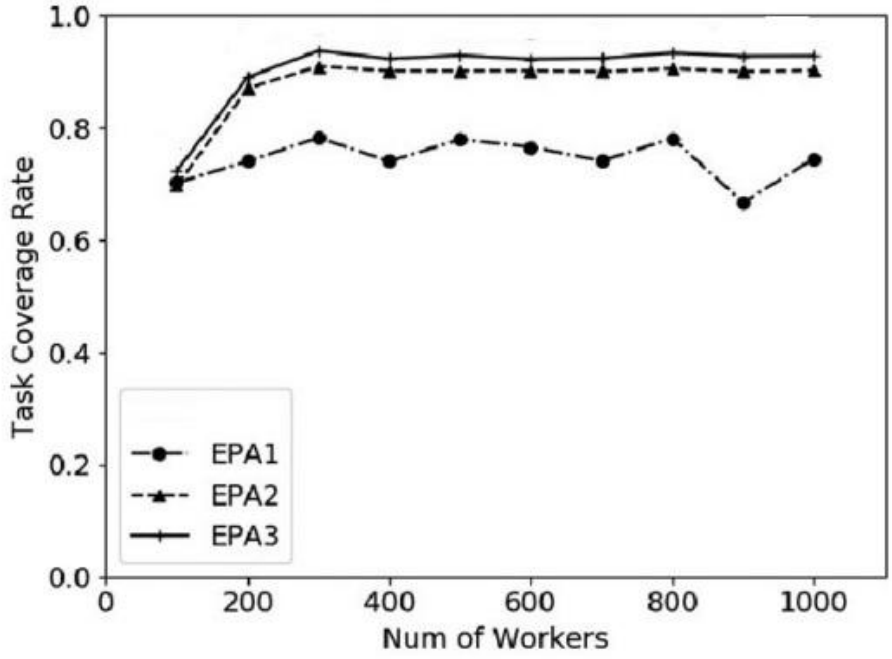

Figure 5: Comparison of Time coverage rate

Figure 5 illustrates the influence of preregistration on both success rate and time cost. To evaluate the impact of the two control parameters, P and Q, one parameter is varied dynamically while keeping the other constant. As depicted in Figure 6(a), when Q = 2, the time cost increases with rising values of P. This occurs because a higher threshold P allows more workers to be accommodated within each subregion, resulting in an average contract success rate exceeding 90%. Conversely, when P = 6 is fixed and Q increases, fewer workers agree to sign contracts due to tighter restrictions on the number of workers per subregion, leading to a reduction in the average success rate. The effect of increasing the number of workers while maintaining fixed subregions on both task coverage and cost is depicted in Figure 6.

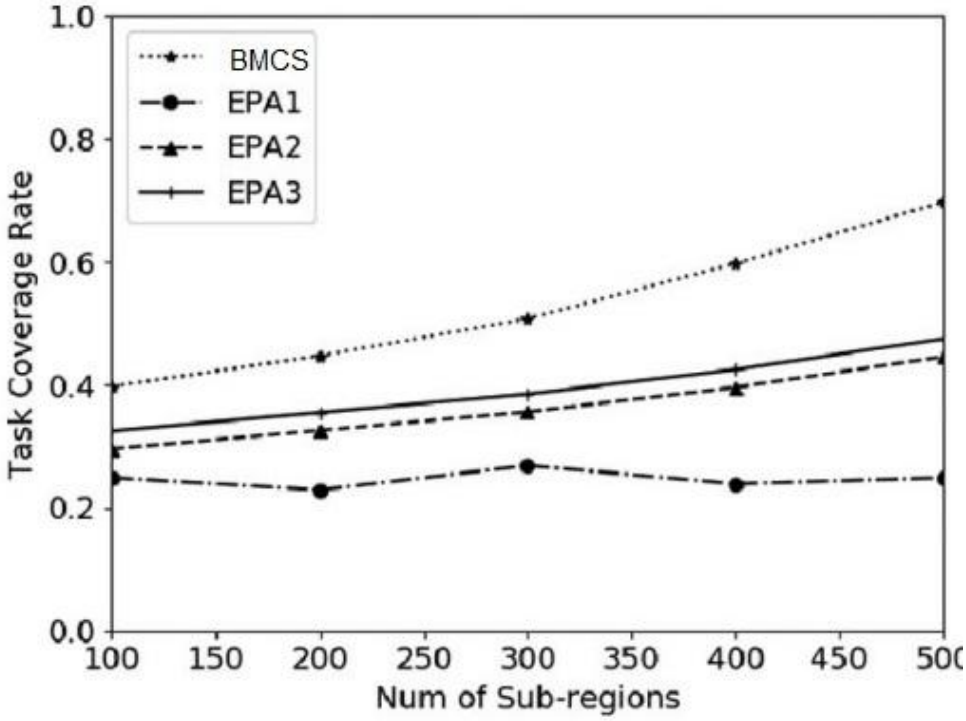

Figure 6: Comparison of Task coverage Rate

Compared to one-step optimization methods (EPA1 and EPA2), our proposed two-step optimization method (EPA3) achieves better result in terms of both task coverage and task cost, which is closer to the result of NPA with no privacy constraint. Since the global optimization of the first stage was taken into account, EPA2 shows a significant improvement than EPA1 in terms of the task coverage rate and efficiency. Based on the fine-tuning optimization in the second stage, EPA3 shows the results closer to the coverage objective. Additional, as shown in Fig. 7(c), increasing the number of workers results in a lower penalized indicator, meaning that EPA3 outperforms the other two approaches, i.e., EPA1 and EPA2.

Our proposed two-step optimization method, EPA3, achieves superior results compared to the one-step optimization methods (EPA1 and EPA2) in terms of task coverage, task cost, and a penalized indicator. Impact of Cloaking Radius: Figure 10 displays the impact of increasing the cloaked radius with a fixed number of workers and subregions on task coverage and cost. The task coverage of EPA1, EPA2, and EPA3 is affected to some extent with the increase in the cloaked radius, except for NPA. However, EPA3 exhibits greater resilience compared to EPA1 and EPA2, indicating that EPA3 is less affected by the cloaked radius. Moreover, EPA3 outperforms the other approaches across all cloaked sizes.

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

DeepScience
Open Access Books

Conclusion

In this article, a location-privacy-preserving MCS system called BMCS was proposed, which incorporates the concept of a blockchain into crowdsensing. This integration facilitates the decentralization of crowdsensing, effectively mitigating security risks such as repudiation and data tampering that are common in traditional centralized systems. Drawing inspiration from smart contracts, we propose a two-phase framework composed of a preregistration phase and a final selection phase. These phases employ spatial location privacy-preserving mechanisms and greedy optimization algorithms to safeguard workers' location information, minimize task costs, and maintain data quality within a blockchain-based crowdsensing model. Moreover, we demonstrate that the optimization problems addressed in both phases are NP-hard. Comprehensive experiments were conducted to evaluate the average block generation time and to compare the proposed approach against two existing schemes. We also examined the influence of various conditions on success rate, execution time, efficiency, and robustness. The results confirm that our method outperforms alternative approaches in terms of operational efficiency, location privacy protection, and task coverage. In future work, we intend to further explore data quality assessment methods to enhance both data reliability and system robustness, thereby improving the model's applicability to real-world deployment scenarios.

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

Acknowledgement

This work was supported by the Universiti Kebangsaan Malaysia under Grant DIP-2018-040.

Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-433-7

References

1. J. Zhang, J. Zhang, Z. Lv and R. Zhang, "On the Security of Privacy-preserving Data Aggregation Scheme Based on CRT in Mobile Crowdsensing System," *2023 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Jiangsu, China, 2023.
2. T. Nestoridis, C. Oikonomou, A. Temperekidis, F. Gioulekas and P. Katsaros, "Scalable IoT architecture for balancing performance and security in mobile crowdsensing systems," *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Paris, France, 2020, pp. 1-8.
3. S. Zou, J. Xi, H. Wang and G. Xu, "CrowdBLPS: A Blockchain-Based Location-Privacy-Preserving Mobile Crowdsensing System," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4206-4218, June 2020.
4. D. M. Kalui, D. Zhang, G. M. Muketha and J. O. Onsomu, "Simulation of Trust-Based Mechanism for Enhancing User Confidence in Mobile Crowdsensing Systems," in *IEEE Access*, vol. 8, pp. 20870-20883, 2020
5. C. Zhao, S. Yang and J. A. McCann, "On the Data Quality in Privacy-Preserving Mobile Crowdsensing Systems with Untruthful Reporting," in *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 647-661, 1 Feb. 2021.
6. C. Zhang, L. Zhu, C. Xu, X. Liu and K. Sharif, "Reliable and Privacy-Preserving Truth Discovery for Mobile Crowdsensing Systems," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1245-1260, 1 May-June 2021
7. X. Dong, Z. You, T. H. Luan, Q. Yao, Y. Shen and J. Ma, "Optimal Mobile Crowdsensing Incentive Under Sensing Inaccuracy," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8032-8043, 15 May15, 2021
8. X. Dong *et al*., "Optimizing Task Location Privacy in Mobile Crowdsensing Systems," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2762-2772, April 2022
9. J. Li, Z. Su, D. Guo, K. -K. R. Choo, Y. Ji and H. Pu, "Secure Data Deduplication Protocol for Edge-Assisted Mobile CrowdSensing Services," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 742-753, Jan. 2021

10. C. Zhang, M. Zhao, L. Zhu, T. Wu and X. Liu, "Enabling Efficient and Strong Privacy-Preserving Truth Discovery in Mobile Crowdsensing," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3569-3581, 2022.
11. B. Zhao, X. Liu, W. -N. Chen and R. H. Deng, "CrowdFL: Privacy-Preserving Mobile Crowdsensing System Via Federated Learning," in *IEEE Transactions on Mobile Computing*, vol. 22, no. 8, pp. 4607-4619, 1 Aug. 2023
12. J. Zhang, P. Li, W. Huang, L. Nie, H. Bao and Q. Liu, "On Privacy-Preserving Task Assignment for Heterogeneous Users in Mobile Crowdsensing," *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Rio de Janeiro, Brazil, 2023, pp. 837-842.
13. J. Wang *et al*., "Personalized Location Privacy Trading in Double Auction for Mobile Crowdsensing," in *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8971-8983, 15 May15, 2023.
14. Y. Jiang, K. Zhang, Y. Qian and L. Zhou, "P2AE: Preserving Privacy, Accuracy, and Efficiency in Location-Dependent Mobile Crowdsensing," in *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2323-2339, 1 April 2023.
15. Y. Cheng, J. Ma, Z. Liu, Y. Wu, K. Wei and C. Dong, "A Lightweight Privacy Preservation Scheme With Efficient Reputation Management for Mobile Crowdsensing in Vehicular Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 1771-1788, 1 May-June 2023.
16. R. Ganjavi and A. R. Sharafat, "Edge-Assisted Public Key Homomorphic Encryption for Preserving Privacy in Mobile Crowdsensing," in *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1107-1117, 1 March-April 2023.
17. B. Zhu, Y. Li, G. Hu and M. Zhang, "A Privacy-Preserving Data Aggregation Scheme Based on Chinese Remainder Theorem in Mobile Crowdsensing System," in *IEEE Systems Journal*, vol. 17, no. 3, pp. 4257-4266, Sept. 2023.
18. Sangeetha, S., Kumari, K.A., Shrinika, M., Sujaybharath, P., Varsini, S.M., Kumar, K.A. (2023). Ensuring Location Privacy in Crowdsensing System Using Blockchain. In: Subhashini, N., Ezra, M.A.G., Liaw, SK. (eds) Futuristic Communication and Network Technologies. VICFCNT 2021. Lecture Notes in Electrical Engineering, vol 995. Springer, Singapore.
19. Payal Chaudhari, “Privacy-preserving cost-effective work distribution with fine-grained access control for mobile crowdsensing”, International Journal of Security and Networks, Vol. 18, No. 2, pp. 106-116, 2023.
20. Y. Cheng *et al*., "A Privacy-Preserving and Reputation-Based Truth Discovery Framework in Mobile Crowdsensing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 5293-5311, Nov.-Dec. 2023.
21. Yujie Liu, Shangping Wang, Duo Zhang, Qian Zhang, Jifang Wang, Optimal incentive strategy in blockchain-based mobile crowdsensing using game theory, Computer Networks, Volume 237, 2023, 110053.

22. Vincenzo Agate, Pierluca Ferraro, Giuseppe Lo Re, Sajal K. Das, BLIND: A privacy preserving truth discovery system for mobile crowdsensing, Journal of Network and Computer Applications, Volume 223, 2024, 103811.