Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **8**, Number **1**, February **2023**

Location Privacy Protection MCS system Based on Double Blockchains

Xiuwen Huang[1], Jiahui Chen[1], Huiwu Huang[1,*], Anar Aliyev[2]

[1] School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China
631813753@qq.com, csjhchen@gmail.com, hedy@gdut.edu.cn
[2] Department of International Relations, Nisantasi University
anar.aliyev@nisantasi.edu.tr

*Corresponding author: Huiwu Huang

Received October 5, 2022, revised November 20, 2022, accepted January 5, 2023.

Abstract.

Crowd sensing allows employees to use mobile devices to collect data at a specific location and send to the requester. However, most existing crowd sensing systems are based on centralized servers which may be attacked, hacked, or manipulated. At the same time, the worker is usually exposed while sends information, which increases the risk of privacy invasion. In order to solve above problems, based on double-blockchains, this paper proposes an efficient model for location privacy protection. Firstly, the new model can resist three kinds of location disclosure in mobile crowd sensing system. Secondly, the proposed model achieves non-repudiation and non-tampering of information function. Thirdly, a two-stage method (i.e., double-blockchains pre-registration and final selection) has advantages of improving data sensing quality, protecting workers' privacy, and improving the efficiency of the model. Finally, we give analysis of the proposed system model to verify its efficiency, feasibility, fairness and reliability.

Keywords: Crowd sensing, location privacy, public blockchain, consortium blockchains, crowd sensing model

1. Introduction.

Recently, wireless sensors have become an emerging application on the Internet of Things (IoT) [1, 2, 3, 4, 5, 6], which enables mobile devices to collect and share data [7, 8, 9]. Collecting relevant data in the region can infer the occurrences within a certain time. This method is called Crowd Sensing [10]. Meanwhile, Spatial crowd sensing (SC) has also been widely used in real-world applications, such as traffic monitor [11, 12], environmental monitor [13], and identification of points of interest [14, 15]. Thereafter, with the development of 5G [16, 17, 18, 19], Wi-Fi and other kinds of mobile communication technologies [20], intelligent mobile terminals play more and more powerful roles in sensing system. In this situation, Mobile Crowd Sensing (MCS) [21, 22, 23] has become a new sensing paradigm for IoT. Generally, MCS services are adopted in air pollution monitoring [24], environmental monitoring [25], road condition monitoring [26], real-time traffic monitoring and navigation [27], healthy diet [28] and autopilot [29], etc. Survey [30] classifies the basic algorithms in MCS environment from the view of task processing and report processing. It also discusses some suitable application scenarios of each algorithm. For the problem of large amount of redundant data in MCS service, Liu et al. [21] describes the current research progress from reducing resource cost and improving service quality points. They also summarize the challenges and technical difficulties existing in

MCS service. Restuccia et al. [31] summarizes the existing research results from three aspects: truth discovery framework, truth discovery algorithm and privacy protection truth discovery algorithm. All these aspects aims at improving MCS data information quality.

However, there are several issues still required to be solved in center-based MCS system. On the one hand, malicious attackers can tamper with information by attacking the centralized system [32, 33]. Therefore, a sensing platform needs a protection mechanism to minimize the risk of privacy leakage [34]. To address this issue, there are three methods (i.e., differential privacy, spatial anonymity and encryption [35, 36, 37]) were proposed in typical privacy protection models in MCS system. For instance, Wang et al. [38] proposed a protection framework based on differential privacy. Workers in spatial crowd sensing first submit their real location information to a trusted mobile service provider, which constructs private spatial decomposition (PSD) and uses Laplace mechanism to achieve differential privacy protection. The work [39] considers spatial location privacy in P2P communication environment, and the P2P spatial K-anonymity algorithm [40] is adopted to achieve the location privacy protection of spatial crowd sensing workers. Yao et al. [41] firstly presented a new encryption protocol based on additive homomorphic encryption technology and garbled circuit to build a secure encryption database for storing workers' location information. However, all the above-mentioned researches still need centralized parties, which cause the mistrust problem.

To tackle the problem of mistrust of centralized platform in real life, we propose a double-blockchains-based MCS system, which not only ensures privacy [42, 43, 44], but also ensures distribution with the addition of multiple consortium blockchains [45, 46, 47, 48]. It ensures that the information in MCS will not be tampered with and can resist malicious acts such as plagiarism and fraud.

The main contributions of this paper are summarized as follows:

- We describe three stages of location privacy exposure in traditional MCS systems and give related attacks of malicious acts for these stages. Then, our proposed framework can resist the mentioned attacks in these three stages.
- Different from other crowd sensing systems, based on cryptography technology, our double-blockchains MCS system can establish a trusted consensus mechanism to avoid security problems (e.g., tampering information). The consortium blockchains can effectively improve the operational efficiency of the whole system. Besides, our framework considers several optimization strategies that can ensure the fairness of workers' choice and further improve efficiency.
- Finally, theoretical analysis of our proposed system proves that it can supply privacy protection. Furthermore, we discussed that the proposed system is more efficient and fair than other baseline blockchain-based systems.

The remainder of this article is organized as follows. We review and summarize the existing works in Section 2. A comprehensive definition is given in Section 3. We present the proposed method and effective algorithm in Section 4. Then, we analyze the performance of our proposed system in detail in Section 5. Finally, Section 6 concludes this paper.

2. **Preliminaries.**

2.1. **System model.**

We begin with the workflow of spatial crowd sensing shown in Figure. 1 as follows:

1. The requester sends the task to the server.
2. Spatial crowd sensing (SC) server obtains location information from workers who accept task requests.

3. SC sensing server assigns tasks to workers according to task location.
4. Once the worker agrees to finish the task, he/she will go to the location where the requester publishes the task. Then, he/she finishes the task and then reports the execution result to SC server.
5. SC server returns results to the requester and evaluates the quality of these results according to a certain mechanism.
6. The requester sends rewards to the workers based on the task results' evaluation.

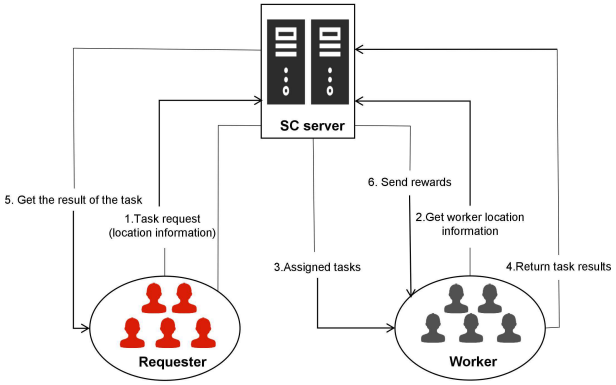

FIGURE 1. Spatial crowd sensing workflow.

Then, as shown in Figure. 2, the MCS system model is mainly composed of three parts: aware user, aware platform and service provider.

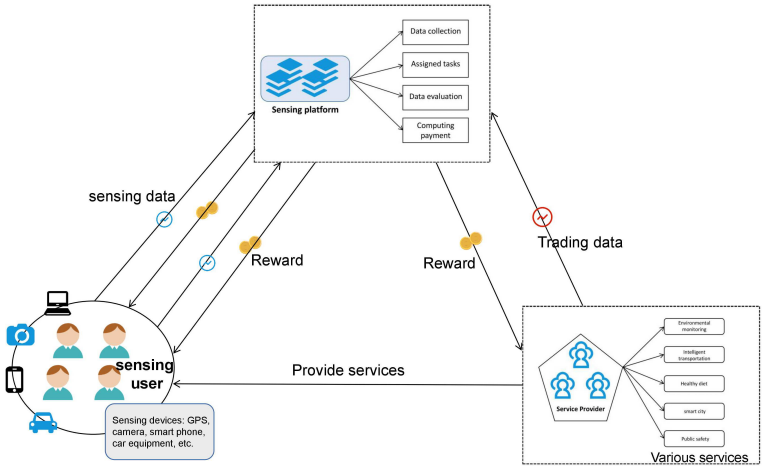

FIGURE 2. Mobile crowd sensing (MCS) system model.

Sensing user. Sensing users are the objects who use intelligent mobile terminals. Their mobile intelligent terminals (e.g., smartphones, tablet computers, wearable devices, and vehicle-mounted sensing devices) are played as basic sensing units. After completing identity authentication, sensing users can use various sensing terminals to collect data, connect with the sensing platform, and report the sensing data.

Sensing platform. As an intermediary between sensing users and service providers, the sensing platform consists of multiple sensing servers. The sensing platform aims at encouraging as many as possible sensing users to participate in the task according to reasonable incentive mechanism. It also deals with the sensing data uploaded by sensing users (e.g., classification, aggregation, and modeling). In general, there are task allocation

algorithms, data processing algorithms, data quality assessment algorithms and reward calculation algorithms adopted in sensing platform.

Service provider. As the requester of sensed data, the security transaction of sensed data is completed by interacting with the sensed platform. The service can be hosted on cloud platforms. It also manages and analyzes the collected sensing data according to sensing data set, and then builds a variety of crowd sensing application. Finally, MCS services are provided for air pollution monitoring, environmental monitoring, road condition monitoring, real-time traffic prediction, healthy diet and safe driving.

2.2. **Basic definition.**

Let $W = \{W_1, W_2, ..., W_n\}$ be the set of workers, and $T = \{t_1, t_2, ..., t_n\}$ be a collection of tasks. More symbols are shown in Table 1 [49].

Table 1. Parameter definition table

Number	Parameter	Define
1	r	Task Requester
2	W	Workers set
3	v	Verifier
4	t_j	Subtarget j
5	n	Number of workers
6	m	Number of subtargets
7	b_i	Worker i budget
8	L_i	Position of worker i
9	A_i	Cloaked area of worker i
10	k_j	Number of workers covered by target j
11	g	Task coverage goal
12	$d_{i,j}$	Euclidean distance from i to j
13	Fm	The matrix results of the first stage
14	Sm	The matrix results of the second stage
15	U	Region coverage matrix
16	S	All areas of the operating range
17	S'	The sub-area overlaps with the surrounding area

Definition 2.2.1. (Cloaked area) To protect the real location, we replace the exact location of worker W_i with the hidden area A_i. Among them, A_i is a spatial anonymous region which formed by mapping the real location of W_i according to the probability density function f_i.

Definition 2.2.2. (Target subregion) To maximize the coverage of task as much as possible, the whole task area S is divided into several sub-areas S_j by the latitude and longitude information. Similarly, the target t is also divided into some sub-targets t_j. Then, if the full coverage of sub-targets in each sub-area is achieved, and the full coverage of targets in the whole task area S is finally achieved.

Definition 2.2.3. (Worker selection) Worker selection can be regarded as mapping worker W_i to subregion S_j, which can be represented by a boolean matrix $Fm_{i,j}$,where $i \in N$ and $j \in M$. If $Fm_{i,j}$=1, it means that worker W_i works in subregion S_j. Conversely, if $Fm_{i,j}$=0, it means that the worker W_i is not working in subregion S_j.

Definition 2.2.4. (Task coverage) Sub-area coverage is defined as the ratio of a worker's work area to sub-area area, which can be described as $\frac{\Sigma_{i \in N}(Fm_{i,j} \times S_{i,j})}{S_j}$, where $Fm_{i,j} \times S_{i,j}$ is

the sub-area working range of W_i. Thus, all overall mission coverage (ATC) is represented as follows:

$$ATC = \Sigma_{j \in M} \frac{\Sigma_{i \in N}(Fm_{i,j} \times S_{i,j})}{S_j}. \tag{1}$$

Definition 2.2.5. (Task cost) We use Euclidean distance to describes the spending in task cost and express it by **d**. Thus, the overall task cost (OTC) is expressed as follows:

$$OTC = \Sigma_{j \in M} \Sigma_{i \in N}(Fm_{i,j} \times d_{i,j}). \tag{2}$$

After a requester r publishes a task, if a worker wants to accept the task, the worker's personal and work information will be sent to the requester through blockchain. The above process is sent to the requester by initiating a transaction. The work requires paying a certain deposit for signing the contract. At the same time, the system should consider the prevention of over-saturation of workers in sub-regions, the coverage of global tasks, the quality of workers in the pre-registration process and the fairness of worker selection.

Definition 2.2.6. (Pre-registration) The first parameter G is a threshold for the number of workers in a same subregion[1]. The second parameter H is the multiple of task coverage target, which aims to improve the success rate of employee selection. The third parameter T is the waiting time of the worker. If T is greater than the parameter $Tmin$, the worker will be selected[2]. When T is greater than the parameter $Tmax$, the legal workers in A_i must be selected. In addition, g is the coverage target set by the system, and its value range is $[0, 1]$.

$$\begin{aligned} \forall i \in N, Pi = \begin{cases} 0, & T_i < Tmin \\ \dfrac{Ti}{Tmax}, & Tmin \leq Ti \leq Tmax \\ 1, & T_i > Tmax \end{cases}, \\ \forall j \in M, Fm_{i,j} \leq G_j, \Sigma_{i \in N}(Fm_{i,j} \times S_{i,j}) \geq H \times g \times S. \end{aligned} \tag{3}$$

Definition 2.2.7. (Local worker selection mechanism, LWSM [49]) Under the condition of ensuring the fairness during worker selection, the goal of LWSM is to achieve subarea coverage optimization with minimal task cost. The greedy algorithm can be used to select the most suitable workers in the subarea.

$$\begin{aligned} max \quad & \Sigma_{j \in M} \Sigma_{i \in N}(\frac{Fm_{i,j} \times S_{i,j}}{S_j} \times \frac{T_i}{24}) \\ s.t. \quad & \forall i \in N, \Sigma_{j \in M}(Fm_{i,j} \times d_{i,j}) \leq b_i \\ & d_{i,j} \geq 0, i \in [1, .., n]; j \in [1, .., m], \end{aligned} \tag{4}$$

However, sub-region optimal does not mean global optimal, and the overall coverage may be low in the case of sub-region optimal. Therefore, after the sub-area optimization stage is completed, the system also needs to optimize the global worker selection process.

Definition 2.2.8. (Global worker selection mechanism, GWSM [49]) Under the condition of ensuring the fairness during worker selection, the goal of GWSM is to achieve global coverage optimization with minimum task cost. The global impact of worker nodes can be calculated according to the proportion of the area where workers work in each surrounding sub-area, and the greedy algorithm can be used to find the most suitable workers globally. While selecting the results of W_i are divided in the task, $Fm_{i,j}$=1. We define $S'_{i,j}$ as the

[1]In other words, it means the maximum number of workers in a subregion.

[2]The greater T is, the higher probability (Pi) of the worker being selected.

overlap between other workers in the sub-areas and the surrounding sub-areas. If $\exists$ $Fm_{k,j}$=1, $i \in N$, and $S'_{k,j} < S'_{i,j}$, then $Fm_{k,j} \leftarrow 1$ and $Fm_{i,j} \leftarrow 0$.

$$\begin{aligned} min \quad & \Sigma_{j\in M}\Sigma_{i\in N}(\frac{24}{T_i} \times Fm_{i,j} \times d_{i,j}), S'_i, j \\ s.t. \quad & \Sigma_{j\in M}\frac{(Fm_{i,j} \times S_{i,j})}{S_j} \geq gS \\ & \forall i \in N, \Sigma_{j\in M}(Fm_{i,j} \times d_{i,j}) \leq b_i \\ & d_{i,j} \geq 0, i \in [1,..,n]; j \in [1,..,m], \end{aligned} \tag{5}$$

Definition 2.2.9. (Fine-tuning stage) A worker belongs to global optimized set can independently adjust accepted tasks according to smart contracts. Since only workers know their exact positions, workers can use their precise positions to fine-tune the results $Sm_{i,j}$ of LWSM and GWSM and decide whether to accept tasks. If a worker refuses, the system will re-select other workers only in the same subarea.

$$\begin{aligned} min \quad & \Sigma_{j\in M}\Sigma_{i\in N}(\frac{24}{T_i} \times Sm_{i,j} \times d_{i,j}) \\ s.t. \quad & |Sm_i - Fm_i| \leq \alpha \\ & \Sigma_{j\in M}\frac{(Sm_{i,j} \times S_{i,j})}{S_j} \geq \Sigma_{j\in M}\frac{(Fm_{i,j} \times S_{i,j})}{S_j} \\ & \forall i \in N, \Sigma_{j\in M}(Sm_{i,j} \times d_{i,j}) \leq b_i \\ & d_{i,j} \geq 0, i \in [1,..,n]; j \in [1,..,m], \end{aligned} \tag{6}$$

W_i is the i-th worker. Fm_i and Sm_i represent vectors corresponding to different stages. T_i represents the i-th workers' idle time. d_i is a Euclidean distance vector, and b_i represents workers' budget. $|Fm_i - Sm_i|$ represents Hamming distance between Fm_i and Sm_i. And the threshold α is used to ensure that the results of second stage keeps the same as the first stage. In addition, the coverage rate of workers should be greater than or equal to that of the first stage.

2.3. **Threat Model.**

We consider three stages during the execution of the sensing task: sensing, uploading and trading. Each stage faces various attacks of data security and privacy leakage as follows:

- Data sensing.

  a) **Location spoofing attack** [50]. An attacker can track an interested sensing task by monitoring the channel and using fake location to disguise as a reliable source. Then, it submits fake data to attack the sensing platform.

  b) **Background knowledge attack** [21]. The attackers use acquired background information such as the user's activity track and the surrounding environment to predict the location area where the user may appear in a certain period of time, and then they may steal more privacy information.
- Data upload.

  a) **Time correlation attack** [51]. By analyzing the uploaded information from one or more locations of a same sensing user in a period of time, the attackers can obtain some activity track of the user. In the worst case, the attacker can infer sensitive information (e.g., the real location and identity) of the sensing user.

  b) **Task-specific attack** [52]. An attacker listens and steals the user's location, identity, and other sensitive information.

c) **Location spoofing attack** [50]. The attackers can monitor and track the interested sensing task through the channel. They may use the false location of the third-party program to disguise as a reliable source, and submit false data to attack the sensing platform.

- Data trading.

a) **Collusion attack** [50]. In this situation, an attacker will collude with the perception platform or service providers. If attacker gets session information of network users, he/she can access to the user background knowledge, then excavate the user's sensitive information further. This case will finally form a malicious interaction process.

b) **Time correlation attack** [51]. In this situation, attackers obtain the sensitive information by analyzing one or more interactions of the same sensing user in a specific period of time. In the most serious case, only a single information interaction can reveal the privacy of the aware user.

3. Our Proposed System Based on Blockchains.

3.1. The Framework.

To solve the workers' privacy issues we mentioned above, a new MCS framework based on double-blockchains system is proposed. The framework is shown in Figure. 3 [53]:

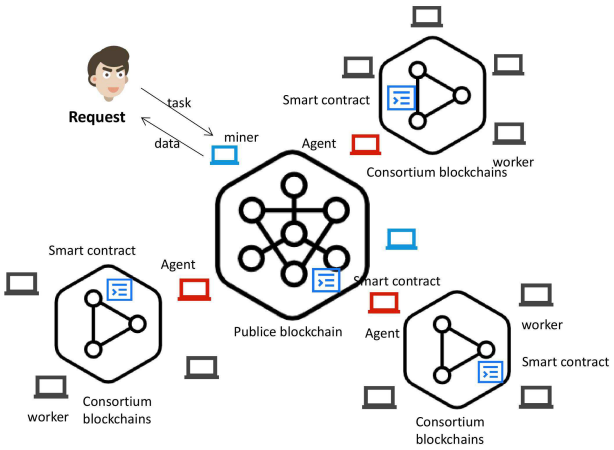

FIGURE 3. The framework of double-blockchains based crowd sensing system.

Requester. Requester r publishes the task on the blockchain. r obtains required awareness data through smart contracts.

Miner. Miners are responsible for verifying the authenticity of transactions. After verification, the transactions will be recorded in the block and miners will get rewarded. As special nodes in the blockchain, miner can also be task requester, agent, or worker.

Agent. The agents are selected from all miners and can organize a consortium blockchain (i.e., divided sub-regions). All participants in the global region can join the public blockchain, but can only participate in the consortium blockchain after successfully registering in the pre-registration phase. The agent downloads sub-target tasks from the public blockchain and publishes them to the agent's affiliate chain network. The agent can charge a deposit to the worker who receives the task.

Worker. Workers are participants who finish tasks. To ensure the fairness of worker selection, we stipulate that the longer the idle time of workers, the higher the probability of workers will be selected.

3.2. **The working phase.**

To better describe the crowd sensing communication process in detail, we define the following eight phases in the double-stranded MSC system (as shown in Figure. 4).

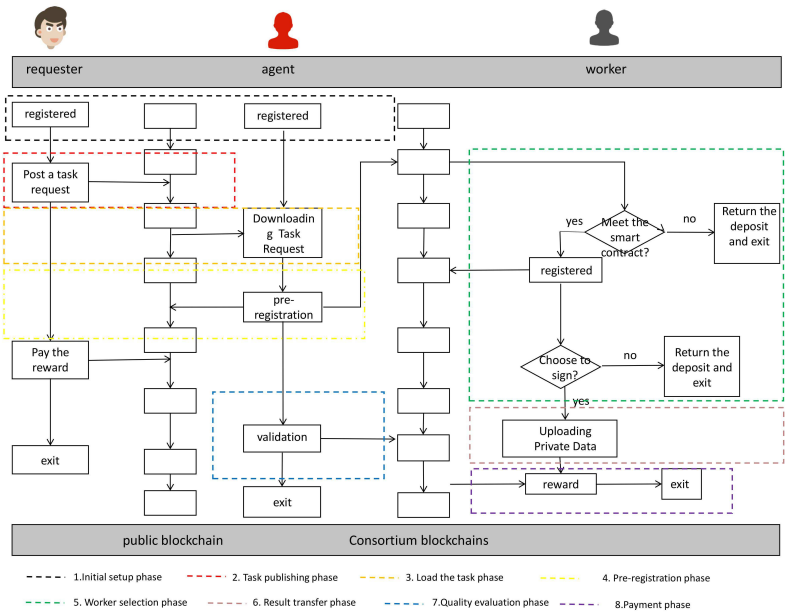

FIGURE 4. MCS execution process based on double-blockchain.

1. **Initial setup phase**: requester and workers have to register in the public blockchain system first, and each registered user will be assigned a pair of public and private key pair. Public and private keys are randomly assigned as a registered user's identity. Only registered users can use blockchain to see relevant task information.
2. **Task publishing phase**: Requester publishes the task with his/her public key in public blockchain to form a transaction. The public key is used to verify the authenticity and validity of the blockchain. At the same time, the smart contract uses the public key to generate the address of the transaction.
3. **Task loading phase**: An agent will be selected from workers. The agent downloads mission information from the public blockchain and then transmits it to its consortium blockchains network. The agent is responsible for ensuring the consistency of mission information between the public and consortium blockchains.
4. **Pre-registration phase**: Workers complete the perception task by initiating transactions on public blockchain. If workers fail to pre-register, they will be rejected to accept the task by the system. Otherwise, workers will join in the final selection process. Only workers who are pre-registered will be accessed into the consortium blockchain. Each consortium blockchain will maintain a successful pre-registered work set.
5. **Worker selection phase:** The worker selection phase is divided into two parts, the optimization of worker selection and the fine-tuning. Once the pre-registration process has done, regions are divided into several subregions. With the condition of fairness of worker selection, the subarea coverage is optimized with the minimum task cost. Then, the global most suitable workers are selected. The selected workers can independently adjust the tasks by themselves. After finish task, workers will not

only obtain reward but also their idle time will be reset. The system selects optimal workers from their corresponding subregions. The number of workers in the final set is equal to the number of workers in the global optimal set. We use WSMC to select suitable workers from the pre-registered staff pool.

6. **Result transmission phase**: After workers complete their tasks, the sensing results with digital signatures and public keys will be uploaded to the public blockchain.
7. **Quality evaluation phase**: The requester will evaluate data quality of task result information. The task result information will be classified into qualified and unqualified groups.
8. **Payment phase**: Workers who upload qualified task data will be rewarded. The requester will automatically pay his/her reward through the smart contract.

4. **The Core Algorithms.**

Algorithm for registering with the public blockchain: As shown in Algorithm 1, task requester and workers are required to register in the public blockchain system, but do not need to provide real identity. Public and private keys for all registered users will be as their identity.

Algorithm 1 Register on a public blockchain

Require: U_{type}
Ensure: pk, sk,U_{id},*RegisterSucess*
1: *RegisterSucess* = False;
2: $\{pk, sk\} \leftarrow$ keyGenerator();
3: $U_{id} \leftarrow pk$;
4: $U_{type} \in$ {Worker, Requester};
5: **if** $U_{id} \in U_{pool}$ **then**
6: **return** *RegisterSucess*
7: **end if**
8: $U_{pool} \leftarrow U_{pool} \cup \{U_{id}\}$;
9: *RegisterSucess*=True;
10: **return** *RegisterSucess*

Line 1 indicates that the flag for successful registration is set to Flase;, lines 2-3 indicate that the key pair is generated, and line 4 indicates the type of registered user (worker or requester) for the user id;; lines 5-10 indicate that if the user id exists in the user pool, the user registration fails, otherwise the user id joins the user pool and the registration is successful.

Algorithm for building Smart Contracts: To ensure the fairness of the transaction, as shown in Algorithm 2, requester creates a smart contract, and any employee who meets the requirements can sign the contract.

Lines 1-2 are initialization parameter settings, lines 3-7 indicate that contract creation fails if the reward is less than task reward; lines 8-15 represent the process of workers verifying success; lines 16 indicate workers' privacy data; lines 17-24 indicate whether the privacy data is appropriate, and select workers to succeed, otherwise fail; lines 25-31 indicate that the task takes time to determine whether the task has been created or not.

Algorithm in pre-registration stage: Considering the worker's work area and global task coverage objectives, we added a pre-registration phase before the worker selection phase. The job information of each worker include the scope of work and spare time. Due to the uneven distribution of workers, some subareas will have dense distribution of workers, while some subareas are short of workers. This causes the coverage target cannot be reached. All of these factors will lead to a decrease in the probability of mission success

Algorithm 2 Building Smart Contracts

Require: W_{id} – The worker's ID, R_{id} – The requester's ID, U_{pool} – User pool, T_{ex} – Task expiration time, T_{id} – The task ID
Ensure: *Status* – Task status

Initialize the value of the *task* ← T_{id}, *Owner* ← R_{id}, *Status* ← Available, *RejectFlag* ← False, *LegalFlag* ← False;
Reward ← setReward(R_{id});
if *Reward* < R_t **then**
    CreateContract ← Failure;
    R_{id} ← Transfer{*Reward*, *Deposit*, *Owner*};
    return *CreateContract*
end if
if Validation(W_{id}) == True and *Reject* == False **then**
    LegalFlag ← True;
    Deposit ← setDeposit(W_{id});
    Sign a contract and publish it on the blockchain;
    Reject ← True;
    Status ← UnAvailable;
    return *RejectFlag*
end if
SensoryData ← UploadingData();
while Evaluation(*SensoryData*) **do**
    if Evaluation(*SensoryData*) is Appropriate **then**
        select W_{id}=True;
    else
        select W_{id}=False;
    end if
    W_{id} ← Transfer{*Reward*, *Deposit*, W_{id}};
end while
if *CostTime*>T_{ex} **then**
    Status ← Failure;
    R_{id} ← Transfer{*Reward*, *Deposit*,*Owner*};
else
    Status ← completed;
end if
return *Status*

and data quality. In addition, the workers in some sub-areas are selected very frequently, but the workers in some sub-areas are hardly selected, and the selection of workers does not have a certain fairness principle. Therefore, we propose pre-registration Algorithm 3 based on control parameters G, H and T to ensure data quality and fairness of worker selection.

Algorithm in selection optimization stage: Follows the work of [49], we divided the selection optimization phase into two steps: WSMCf and WSMCs, while considered more parameters for fairness. Firstly, WSMCf combines LWSM and GWSM. It is based on the combination of uncertain location. Secondly, based on exact location information, WSMCs is the fine-tuning stage of WSMCf results, which is fine-tuned on smart contracts in the consortium blockchains.

Step 1 optimization: In the first stage of worker selection, an effective greedy algorithm based on partial set coverage problem was proposed to solve the problem of location uncertainty [54]. We use hidden areas instead of exact location of users to accept tasks.

Algorithm 3 Pre-registration

Require: r_i – The preferred work area for workers,R_i – Sub-region,F – Initialize worker matrix,S_i – The area covered by the worker W_i's task,T_i – Worker W_i's leisure time,S – Task coverage area,g – Task coverage target,Num_i – The number of workers in the subregion,G – The threshold for the number of workers in a subregion,H – The multiple of the task covering the target.

Ensure: F' – Final worker matrix.

if $\Sigma_{i\in N}(F_i \times S_i) < H \times g \times S$ **then**
  if $Num_i < G$ and $r_i \in R_i$ and $T_i \geq Tmin$ **then**
    if $T_i > Tmax$ **then**
      Num_i+=1;
      $F_i \leftarrow 1$;
      Contracts between workers and task requester on a public blockchain;
      if $Tmin \leq T_i \leq Tmax$ **then**
        Calculate the probability of being a worker as P;
        if selected **then**
          Num_i+=1;
          $F_i \leftarrow 1$;
          Contracts between workers and task requesters on a public blockchain;
        end if
      end if
    end if
    $F'_i \leftarrow F_i$;
  end if
end if
return F'_i;

Then, the Euclidean distance is used to evaluate perceived cost between workers and sub-goals.

(1) Geometric centroid point method [49]**:** As shown in Figure. 5, there are numerous location points z uniformly distributed in the hidden region A_i ($z \in A_i$). The geometric centroids of all points in the hidden region are calculated as the expected positions of workers. Finally, the expected distance matrix d is obtained, where l_j represents the position of the target j in the sub-region. $dis()$ function represents the Euclidean distance function.

$$d_{i,j} = dis(\int_{z\in A_i} z f_i(z)dz, l_j). \tag{7}$$

(2) Optimization for the first step [49]**:** We first used a simple pruning method to reduce the hidden area A_i to A'_i. As shown in Figure. 6, the coverage area of target j is a circular area with target j (center) and r_i (radius). A'_i is overlap between the coverage of A_i and j. f_i is a probability density function, which maps the exact location of workers z into a hidden area. The probability of successful access $p_{i,j}$ is calculated as follows:

$$p_{i,j} = \int_{z\in A_i} z f_i(z)dz. \tag{8}$$

According to consider probability of successful access $p_{i,j}$, we can calculate the expected distance $d'_{i,j}$ by the following formula:

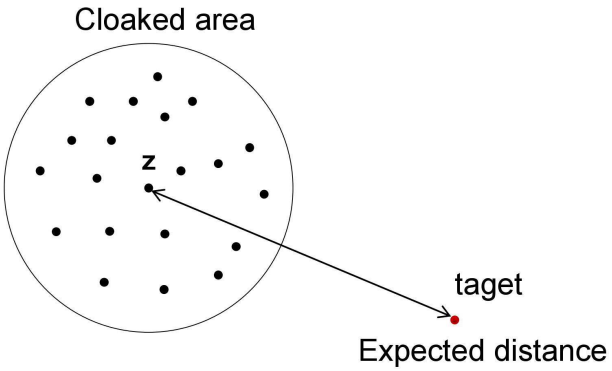

FIGURE 5. Geometric centroid point method.

$$d'_{i,j} = \frac{\int_{z \in A_i} dis(z, l_j) f_i(z) dz}{p_{i,j}}. \tag{9}$$

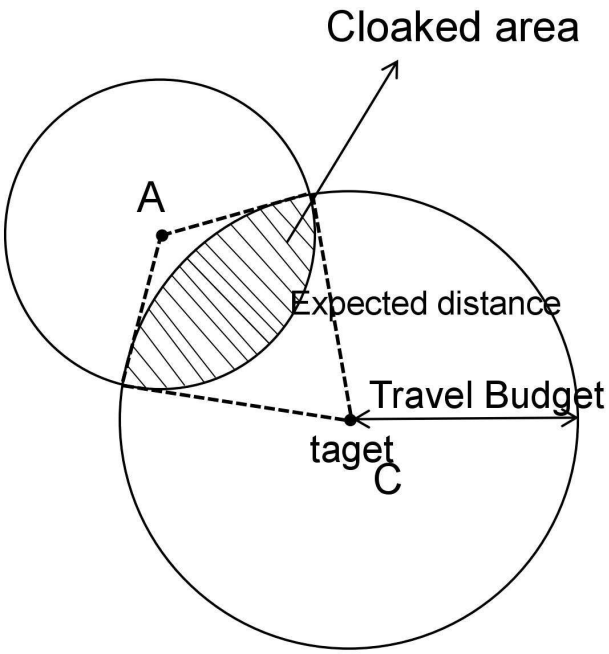

FIGURE 6. Expected probability method.

In the first step, we combine a greedy algorithm to select workers. The system chooses the most efficient workers to work for a subregion and updates the coverage of the subregion target in real time. Once the coverage goal is reached or the worker travel budget is exhausted, the algorithm will terminate. The cost-benefit calculation is as follows:

$$\delta_{i,j}^{(1)} = \frac{d'_{i,j}}{min(1 - U_j, \frac{1}{k_j}) + \alpha}. \tag{10}$$

U represents the matrix vector of the current coverage part of the subregion target. The entire denominator represents the expected coverage contributed by W_i ($U_j = \frac{\Sigma_{i \in N} Fm_{i,j} \times S_{i,j}}{S_j}$). Thus, the expected coverage of the contribution of a worker W_i to the target t_j is

$min(1 - U_j, \frac{1}{k_j})$. The role of α is to prevent over coverage. The proposed algorithm 4 can select appropriate workers. At the same time, an upper threshold R is adopted to stop the algorithm.

Algorithm 4 Fair worker selection algorithm

Require: W – A collection of workers, T_r – The target collection of the subregion, T_i – Worker W_i's leisure time, b – Budget vector, d' – Expected distance matrix, k – Subtarget coverage requirement vector, g – Task coverage target, p – Choice probability matrix, R – The iterative threshold.

Ensure: Fm – The first worker selection matrix, U – Partial vector of target coverage

Fm=0, U=0, ATU=0, r=0;
while $ATU \leq g \times S$ and $r < R$ and $T_i \geq Tmin$ **do**
  if exists suitable workers W_i **then**
    if $T_i \geq Tmax$ **then**
      The probability of successful W_i selection for workers is pi, j;
    end if
    if $T_i < Tmax$ **then**
      The probability of successful W_i selection for workers $p \times pi, j$;
    end if
    if selected **then**
      $Fm_{i,j} \leftarrow 1$;
      $ATU \leftarrow min(1 - U_j, \frac{1}{k_j}) \times S_j + ATU$;
      $U_j \leftarrow min(1 - U_j, \frac{1}{k_j}) \times S_j + U_j$;
      $b_j \leftarrow b_j - d'_{i,j}$;
      if $U_j == 1$ **then**
        $T_r \leftarrow \frac{T_r}{t_j}$;
      end if
      if $b_i == 0$ **then**
        $W \leftarrow \frac{W}{W_i}$;
      end if
    else
      $R \leftarrow R + 1$;
    end if
  else
    break;
  end if
end while

(3) Optimization for the second step [49]**:** In the second step, workers can decide whether to refuse the task. The selected worker may not be able to access the subtarget because of uncertainty of the anonymous location. Therefore, without affecting the overall coverage, the allocation results need to be fine-tuned in the second optimization step.

Algorithm 5 describes the fine-tuning algorithm for the second stage of worker selection. Again, it is given a certain probability to interactively select the appropriate worker W_i to avoid over coverage. Unlike Algorithm 4, we want to satisfy the first constraint of **(6)**.

$$\delta_{i,j}^{(2)} = \frac{\frac{d'_{i,j}}{b_i} + 1 - Fm_{i,j}}{min(1 - U_j, \frac{1}{k_j}) + \alpha}. \tag{11}$$

Similar to Algorithm 4, we use the iteration threshold R' to stop the algorithm. Different from the optimization in the first step, the probability $p'_{i,j}$ in the second step is calculated as follows:

$$p'_{i,j} = 1 - \frac{\delta^{(2)}_{i,j}}{max\delta^{(2)}_{i,j}}. \tag{12}$$

Algorithm 5 Fair fine-tuning algorithm

Require: W – A collection of workers, T_r – The target collection of the subregion, T_i – Worker W_i's leisure time, b – Budget vector, k – Subtarget coverage requirement vector, R' – The iterative threshold, U – Partial vector of target coverage, STU – Select the coverage of workers for the first time, LTU – Select the coverage of workers for the second time.

Ensure: Sm – The second worker selection matrix.

Sm_i=0, LTU=0, STU=0, r=0;
for all subtargets in T_r **do**
  $U_j \leftarrow U_j$ - $\frac{Fm_{i,j}}{k_j}$;
  $STU \leftarrow STU + \frac{Fm_{i,j}}{k_j}$;
end for
while $LTU \leq STU$ and $r < R'$ and $b_i > 0$ $T_i \geq Tmin$ **do**
  if there is a possible subtarget in Tr **then**
    if $T_i \geq Tmax$ **then**
      The probability of successful W_i selection for workers is 1;
    end if
    if $T_i < Tmax$ **then**
      The probability of successful W_i selection for workers is p;
    end if
    if selected **then**
      if $d_{i,j} < b_i$ **then**
        $Sm_{i,j} \leftarrow 1$;
        $LTU \leftarrow min(1 - U_j, \frac{1}{k_j}) \times S_j + LTU$;
        $U_j \leftarrow min(1 - U_j, \frac{1}{k_j}) \times S_j + U_j$;
        $b_j \leftarrow b_j$ - $d_{i,j}$;
        $T_r \leftarrow \frac{T_r}{t_j}$;
      end if
    else
      $R \leftarrow R+1$;
    end if
  else
    break;
  end if
end while

5. Analysis.

Different from the traditional public sense system, there exists leakage of user sensitive information during the registration phase. Our system uses pseudonyms of bitcoin addresses to represent task requester and workers. This protects the privacy of crowd sensing tasks without submitting their real identities. According to the submitted work information, especially the location information, we propose a location privacy protection method based on the spatial hidden area, which replaces the real location area of the

workers with the corresponding hidden area to receive the task information and prevent the workers from being exposed to the public's real location. Therefore, our system can provide dual protection for identity privacy and location privacy. For example, multiple consortium blockchains disperse transaction records and disrupt the original transaction sequence, which can resist traditional time-linked attacks. Table 2 below lists the privacy protection performance of our MCS system compared with other systems.

Table 2. Security comparison table

Whether the system defends against attacks	Location spoofing attack	Background knowledge attack	Time correlation attack	Task specific attack	Conspiracy to attack
Traditional MCS system	×	×	×	×	×
[55]	✓	✓	×	×	✓
CrowdBLPS [49]	✓	✓	×	×	✓
Our system	✓	✓	✓	✓	✓

For the location privacy problem of the traditional MCS system in three stages, our system can well resist this privacy problem. Specifically:

- As for the location spoofing attack in the data sensing stage, because of the decentralized characteristics of blockchain, the privacy problem caused by the centralized sensing platform or service providing disguises to send false information is well resisted. And the anonymity of blockchain can naturally resist background knowledge attacks, too.
- Considering time-related attacks, our system utilizes some consortium blockchains. The corresponding location request interaction runs on the consortium blockchains, which disrupts the order of task information in public blockchain. Thus, it is capable of resisting time-related attacks. In our new system, users upload their work scope in the public blockchain, but do not upload the exact location information. The security of consortium blockchains is higher than that of the public blockchain, so it can resist specific task attacks.
- Due to the decentralized characteristics of the blockchain, the collusion attack caused by the centralized sensing platform or service provider providing perceived user information to the attacker will be well resisted in data transaction stage.

On the one hand, there is no information encryption when users upload their location information, it cannot resist stealing users' locations attacks. On the other hand, it does not disrupt the transaction order. Thus, it cannot resist time correlation attacks. Although the MCS system [53] adopts multiple private blockchains, the user information uploaded in the public blockchain still does not encrypt. It also cannot resist task-specific attack by stealing the user's location. For the CrowdBLPS system [49], although the user's exact location is not uploaded during pre-registration, it has to upload the user's exact location information during the worker selection phase on public blockchain. CrowdBLPS system also cannot disrupt the order of transactions, and makes it vulnerable to time-linked attacks (which are generally secure). Our system solves all above privacy issues mentioned in the appeal well with high security.

Efficiency The traditional systems are efficient because they run fast on local, private, and consortium blockchain [53]. Study [55] and CrowdBLPS system [49] to run the algorithm on the public blockchain and thus takes a long time to reach a consensus.

Our system runs the algorithm on the double-blockchains (i.e., public and consortium blockchains), which combines both advantages of public and consortium blockchains.

Fairness To prevent some eligible workers from remaining idle for a long time., our system adds an idle time parameter T. The longer idle time of worker owns, the higher probability of being selected in stages. The fairness of selecting workers is guaranteed, so the fairness is high; However, the traditional MCS system [55, 53] and CrowdBLPS system [49] do not add the idle time parameter T to the users, which cannot guarantee the fairness of worker selection.

6. Conclusions.

In this paper, we propose a location privacy protection system based on double-chains. The system avoids some security problems such as information denial and tampering in the traditional centralized public sense system. To improve the quality of data sensory and protect workers' privacy, we propose a two-step method with pre-registration and selection. More precisely, to run the pre-registration method on a public blockchain and the fine-tuning method of the selection phase on a consortium blockchain. Since the pre-registration stage only needs to upload the user's work and the consortium blockchains has high efficiency, this can solve the location privacy problem of workers. To improve the efficiency of the model, we adopt multiple consortium blockchains to distribute the transaction records of workers. To improve the service quality of our system, we formalize some parameters in the pre-registration stage to enhance the fairness of worker selection. Finally, we theoretically analyze the system model, and the results show that our system is efficient, feasible, fair, and reliable.

REFERENCES

[1] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (iot)," *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, 2015.

[2] A. Shafiq, M. F. Ayub, K. Mahmood, M. Sadiq, S. Kumari, and C.-M. Chen, "An identity-based anonymous three-party authenticated protocol for iot infrastructure," *Journal of Sensors*, vol. 2020, p. 8829319, 2020.

[3] T.-Y. Wu, T. Wang, Y.-Q. Lee, W. Zheng, S. Kumari, and S. Kumar, "Improved authenticated key agreement scheme for fog-driven iot healthcare system," *Security and Communication Networks*, vol. 2021, p. 6658041, 2021.

[4] C.-M. Chen, X. Li, S. Liu, M.-E. Wu, and S. Kumari, "Enhanced authentication protocol for the internet of things environment," *Security and Communication Networks*, vol. 2022, p. 8543894, 2022.

[5] T.-Y. Wu, L. Wang, X. Guo, Y.-C. Chen, and S.-C. Chu, "Sakap: Sgx-based authentication key agreement protocol in iot-enabled cloud computing," *Sustainability*, vol. 14, no. 17, p. 11054, 2022.

[6] T.-Y. Wu, Q. Meng, S. Kumari, and P. Zhang, "Rotating behind security: A lightweight authentication protocol based on iot-enabled cloud computing environments," *Sensors*, vol. 22, no. 10, p. 3858, 2022.

[7] C.-M. Chen, Z. Chen, S. Kumari, and M.-C. Lin, "Lap-ioht: A lightweight authentication protocol for the internet of health things," *Sensors*, vol. 22, no. 14, p. 5401, 2022.

[8] K. Renuka, S. Kumar, S. Kumari, and C.-M. Chen, "Cryptanalysis and improvement of a privacy-preserving three-factor authentication protocol for wireless sensor networks," *Sensors*, vol. 19, no. 21, p. 4625, 2019.

[9] C.-M. Chen, B. Xiang, T.-Y. Wu, and K.-H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *Applied Sciences*, vol. 8, no. 7, p. 1074, 2018.

[10] H. Ma, D. Zhao, and P. Yuan, "Opportunities in mobile crowd sensing," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 29–35, 2014.

[11] T. Sense, "Rich monitoring of road and traffic conditions using mobile smartphones," Microsoft Research, Tech. Rep. MSR-TR-2008-59, Tech. Rep., 2008.

[12] S.-M. Zhang, X. Su, X.-h. Jiang, M.-l. Chen, and T.-Y. Wu, "A traffic prediction method of bicycle-sharing based on long and short term memory network." *Journal of Network Intelligence*, vol. 4, no. 2, pp. 17–29, 2019.

[13] R. K. Rana, C. T. Chou, S. S. Kanhere, N. Bulusu, and W. Hu, "Ear-phone: an end-to-end participatory urban noise mapping system," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2010, pp. 105–116.

[14] Y. Chon, N. D. Lane, F. Li, H. Cha, and F. Zhao, "Automatically characterizing places with opportunistic crowdsensing using smartphones," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 2012, pp. 481–490.

[15] J. Gao, H. Zou, F. Zhang, and T.-Y. Wu, "An intelligent stage light-based actor identification and positioning system," *International Journal of Information and Computer Security*, vol. 18, no. 1-2, pp. 204–218, 2022.

[16] N. Hassan, K.-L. A. Yau, and C. Wu, "Edge computing in 5g: A review," *IEEE Access*, vol. 7, pp. 127 276–127 289, 2019.

[17] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, "An authenticated key exchange protocol for multi-server architecture in 5g networks," *IEEE Access*, vol. 8, pp. 28 096–28 108, 2020.

[18] L. Yang, Y.-C. Chen, and T.-Y. Wu, "Provably secure client-server key management scheme in 5g networks," *Wireless Communications and Mobile Computing*, vol. 2021, p. 4083199, 2021.

[19] T.-Y. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the security: An enhanced authentication protocol for drone communications over 5g networks," *Drones*, vol. 6, no. 1, p. 10, 2022.

[20] T.-Y. Wu, Q. Meng, L. Yang, X. Guo, and S. Kumari, "A provably secure lightweight authentication protocol in mobile edge computing environments," *The Journal of Supercomputing*, vol. 78, pp. 13 893–13 914, 2022.

[21] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A survey of mobile crowdsensing techniques: A critical component for the internet of things," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 3, pp. 1–26, 2018.

[22] C. Jiang, L. Gao, L. Duan, and J. Huang, "Scalable mobile crowdsensing via peer-to-peer data sharing," *IEEE Transactions on Mobile Computing*, vol. 17, no. 4, pp. 898–912, 2017.

[23] W. Sherchan, P. P. Jayaraman, S. Krishnaswamy, A. Zaslavsky, S. Loke, and A. Sinha, "Using on-the-move mining for mobile crowdsensing," in *2012 IEEE 13th International Conference on Mobile Data Management*. IEEE, 2012, pp. 115–124.

[24] P. Dutta, P. M. Aoki, N. Kumar, A. Mainwaring, C. Myers, W. Willett, and A. Woodruff, "Common sense: participatory urban sensing using a network of handheld air quality monitors," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, 2009, pp. 349–350.

[25] M. Demirbas, C. Rudra, A. Rudra, and M. A. Bayir, "imap: Indirect measurement of air pollution with cellphones," in *2009 IEEE international Conference on Pervasive Computing and Communications*. IEEE, 2009, pp. 1–6.

[26] C.-Y. Lin, L.-J. Chen, Y.-Y. Chen, W.-C. Lee *et al.*, "A comfort measuring system for public transportation systems using participatory phone sensing," *ACM Phonesense*, 2010.

[27] V. Manolopoulos, S. Tao, S. Rodriguez, M. Ismail, and A. Rusu, "Mobitras: A mobile application for a smart traffic system," in *Proceedings of the 8th IEEE International NEWCAS Conference 2010*. IEEE, 2010, pp. 365–368.

[28] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, and M. Hansen, "Image browsing, processing, and clustering for participatory sensing: lessons from a dietsense prototype," in *Proceedings of the 4th Workshop on Embedded Networked Sensors*, 2007, pp. 13–17.

[29] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, and A. T. Campbell, "Bikenet: A mobile sensing system for cyclist experience mapping," *ACM Transactions on Sensor Networks (TOSN)*, vol. 6, no. 1, pp. 1–39, 2010.

[30] I. J. Vergara-Laurens, L. G. Jaimes, and M. A. Labrador, "Privacy-preserving mechanisms for crowdsensing: Survey and research challenges," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 855–869, 2016.

[31] F. Restuccia, N. Ghosh, S. Bhattacharjee, S. K. Das, and T. Melodia, "Quality of information in mobile crowdsensing: Survey and research challenges," *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 4, pp. 1–43, 2017.

[32] L. Pournajaf, D. A. Garcia-Ulloa, L. Xiong, and V. Sunderam, "Participant privacy in mobile crowd sensing task management: A survey of methods and challenges," *ACM Sigmod Record*, vol. 44, no. 4, pp. 23–34, 2016.
[33] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, 2017.
[34] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. H. Deng, "Crowdbc: A blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251–1266, 2018.
[35] T.-Y. Wu, X. Fan, K.-H. Wang, J.-S. Pan, and C.-M. Chen, "Security analysis and improvement on an image encryption algorithm using chebyshev generator," *Journal of Internet Technology*, vol. 20, no. 1, pp. 13–23, 2019.
[36] T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 20–28, 2019.
[37] R. Tso, K. Huang, Y.-C. Chen, S. M. M. Rahman, and T.-Y. Wu, "Generic construction of dual-server public key encryption with keyword search on cloud computing," *IEEE Access*, vol. 8, pp. 152 551–152 564, 2020.
[38] WangQian, YangLiYun, and YangDeLi, "User preference oriented collaborative filtering algorithm for attribute value scoring distribution," *Journal of Systems Engineering*, no. 4, 2010.
[39] J. Hu, L. Huang, L. Li, M. Qi, and W. Yang, "Protecting location privacy in spatial crowdsourcing," in *Asia-Pacific Web Conference*. Springer, 2015, pp. 113–124.
[40] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica*, vol. 15, no. 2, pp. 351–380, 2011.
[41] A. C.-C. Yao, "How to generate and exchange secrets," in *27th Annual Symposium on Foundations of Computer Science (SFCS 1986)*. IEEE, 1986, pp. 162–167.
[42] J. M.-T. Wu, Q. Teng, S. Huda, Y.-C. Chen, and C.-M. Chen, "A privacy frequent itemsets mining framework for collaboration in iot using federated learning," *ACM Transactions on Sensor Networks (TOSN)*, 2022, https://doi.org/10.1145/3532090.
[43] C.-M. Chen, Z. Tie, E. K. Wang, M. K. Khan, S. Kumar, and S. Kumari, "Verifiable dynamic ranked search with forward privacy over encrypted cloud data," *Peer-To-Peer Networking and Applications*, vol. 14, no. 5, pp. 2977–2991, 2021.
[44] Z. Bao, W. Shi, S. Kumari, Z.-y. Kong, and C.-M. Chen, "Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity," *International Journal of Information Security*, vol. 19, no. 3, pp. 311–321, 2020.
[45] C.-M. Chen, X. Deng, W. Gan, J. Chen, and S. Islam, "A secure blockchain-based group key agreement protocol for iot," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 9046–9068, 2021.
[46] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C.-M. Chen, "An improved blockchain-based authentication protocol for iot network management," *Security and Communication Networks*, vol. 2020, p. 8836214, 2020.
[47] Q. Mei, H. Xiong, Y.-C. Chen, and C.-M. Chen, "Blockchain-enabled privacy-preserving authentication mechanism for transportation cps with cloud-edge computing," *IEEE Transactions on Engineering Management*, 2022, https://doi.org/10.1109/TEM.2022.3159311.
[48] C.-M. Chen, X. Deng, S. Kumar, S. Kumari, and S. Islam, "Blockchain-based medical data sharing schedule guaranteeing security of individual entities," *Journal of Ambient Intelligence and Humanized Computing*, 2021, https://doi.org/10.1007/s12652-021-03448-7.
[49] S. Zou, J. Xi, H. Wang, and G. Xu, "Crowdblps: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4206–4218, 2019.
[50] T. Zhou, Z. Cai, K. Wu, Y. Chen, and M. Xu, "Fidc: A framework for improving data credibility in mobile crowdsensing," *Computer Networks*, vol. 120, pp. 157–169, 2017.
[51] B. Niu, Y. Chen, Z. Wang, F. Li, B. Wang, and H. Li, "Eclipse: Preserving differential location privacy against long-term observation attacks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 1, pp. 125–138, 2020.
[52] L. Hu and C. Shahabi, "Privacy assurance in mobile sensing networks: Go beyond trusted servers," in *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 2010, pp. 613–619.

[53] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Generation Computer Systems*, vol. 94, pp. 408–418, 2019.
[54] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017, pp. 557–564.
[55] H. Wang, C. Wang, Z. Shen, K. Liu, P. Liu, and D. Lin, "A madm location privacy protection method based on blockchain," *IEEE Access*, vol. 9, pp. 27 802–27 812, 2021.